

# Introduction to Computer Crime

**M. E. Kabay, PhD, CISSP-ISSMP**  
**Program Director, MSIA**  
**School of Graduate Studies**  
**Norwich University**  
**Northfield, VT**

# Introduction to Computer Crime

by M. E. Kabay, PhD, CISSP-ISSMP  
Program Director, MSIA  
School of Graduate Studies  
Norwich University, Northfield VT

*Much of the following material was originally published in the 1996 textbook,  
NCSA Guide to Enterprise Security (McGraw Hill) and was most recently updated with newer references  
for use in Norwich University programs in July 2006.*

Introduction to Computer Crime.....	1
1 Sabotage: Albert the Saboteur .....	3
2 Piggybacking.....	4
3 Impersonation .....	7
4 Equity Funding Fraud .....	8
4.1 What happened.....	8
4.2 Lessons.....	8
5 Superzapping.....	10
6 Scavenging: Garbage Out, Data In .....	12
6.1 Legal status of garbage .....	12
6.2 RAM and Virtual Memory.....	13
6.3 Magnetic Spoor.....	13
6.4 Bye-Bye, Data.....	14
7 Trojan horses.....	16
7.1 Case studies.....	16
7.2 1993-1994: Internet monitoring attacks.....	17
7.3 Cases from the INFOSEC Year in Review Database .....	18
7.4 Hardware Trojans.....	23
7.5 Diagnosis and prevention.....	24
8 Back Doors: Secret Access .....	25
8.1 Origins.....	25
8.2 Examples of Back Doors .....	25
8.3 Easter Eggs and the Trusted Computing Base .....	26
8.4 Back Doors: RATs.....	28
8.5 Back Doors: Testing Source Code.....	29
8.6 Additional resources .....	30
8.7 Additional reports .....	30

9	Voice Mail Security .....	36
10	Salami Fraud .....	38
11	Logic bombs.....	40
11.1	Time bombs .....	40
11.2	Renewable software licenses .....	40
11.3	Circumventing logic bombs.....	42
12	Data leakage.....	43
12.1	Some cases of data leakage:.....	44
12.2	USB Flash Drives .....	50
12.3	Surveillance.....	52
12.4	Steganography.....	53
12.5	Inference .....	53
12.6	Plugging covert channels .....	53
13	Extortion .....	55
13.1	More recent cases:.....	55
13.2	Defenses .....	58
14	Forgery .....	59
14.1	Desktop forgery .....	59
14.2	Fake credit cards .....	60
15	Simulation.....	62
16	References.....	63

## **1 Sabotage: Albert the Saboteur**

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.

## 2 Piggybacking

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.

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/netoff.asp> > 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 shutdown.

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.

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.<sup>1</sup>

---

<sup>1</sup> For a discussion of proximity devices to prevent piggybacking, see Kabay, M. E. (2004). The end of passwords: Ensure's approach, Part 1 < <http://www.networkworld.com/newsletters/sec/2004/0607sec1.html> > and Part 2 < <http://www.networkworld.com/newsletters/sec/2004/0607sec2.html> >

### 3 Impersonation

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 drop-off 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.”



## **4 Equity Funding Fraud**

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.

### **4.1 What happened**

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 dizzily 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.

### **4.2 Lessons**

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.

## 5 Superzapping

“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?

- Privileged debuggers: tools which allow unrestricted access to memory and disk structures;
- Disk editors: permit any change to be written to disk without passing through the file system;
- Program patchers: modify executable program files without having to recompile source code;
- Database tools: can change portions of a database without regard for logical consistency;
- Spoolfile editors: modify output files before printing;
- 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.

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 as 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.

## 6 Scavenging: Garbage Out, Data In

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).

### 6.1 Legal status of garbage

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.

*NewsScan* authors John Gehl and Suzanne Douglas summarized the rest of the story as follows: In mid-2000,

Microsoft . . . [complained] that various organizations allied to it have been victimized by industrial espionage agents who attempted to steal documents from trash bins. The organizations include the Association for Competitive Technology in Washington, D.C., the Independent Institute in Oakland, California, and Citizens for a Sound Economy, another Wash., D.C.-based entity. Microsoft . . . [said], “We have sort of always known that our competitors have been actively engaged in trying to define us, and sort of attack us. But these revelations are particularly concerning and really show the lengths to which they’re willing to go to attack Microsoft.” (*Washington Post* 20 Jun 2000)

Saying he was exercising a “civic duty,” Oracle chairman and founder Lawrence J. Ellison defended his company of suggestions that Oracle’s behavior was “Nixonian” when it hired private detectives to scrutinize organizations that supported Microsoft’s side in the antitrust suit brought against it by the government. The investigators went through trash from those organizations in attempts to find information that would show that the organizations were controlled by Microsoft. Ellison, who, like his nemesis Bill Gates at Microsoft, is a billionaire, said, “All we did was to try to take information that was hidden and bring it into the light,” and added: “We will ship our garbage to [Microsoft], and they can go through it. We believe in full disclosure.” “The only thing more disturbing than Oracle’s behavior is their ongoing attempt to justify these actions,” Microsoft said in a statement. “Mr. Ellison now appears to acknowledge that he was personally aware of and personally authorized the broad overall strategy of a covert operation against a variety of trade associations.” (*New York Times* 29 Jun 2000)

Discarded information can reside on paper, magnetic disks and tapes, and even electronic media such as PC-card ram disks. 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.

At this point, 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.

## 6.2 RAM and Virtual Memory

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.

## 6.3 Magnetic Spoor

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.

*Quick formatting* a disk drive reinitializes file system structures such as the file allocation table but leaves the raw file data untouched. Full formatting using the operating system is a *high-level* format that leaves data in a recoverable state. *Low-level* formatting is normally carried out at the factory and establishes sectors, cylinders and address information for accessing the drive. Low-level formatting may render all data previously stored on a disk inaccessible to the operating system but not necessarily to specialized recovery programs.

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.

## 6.4 Bye-Bye, Data

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 WipeDrive < <http://www.whitecanyon.com/wipedrive.php> >. 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, ah, carrion when data scavengers steal our secrets.



## 7 Trojan horses

Some of my younger students have expressed bewilderment over the term Trojan “horse.” They associate “Trojan” with condoms and with evil programs. Here’s the original story:

...But Troy still held out, and the Greeks began to despair of ever subduing it by force, and by advice of Ulysses resolved to resort to stratagem. The Greeks then constructed an immense wooden horse, which they gave out was intended as a propitiatory offering to Minerva, but in fact was filled with armed men. The remaining Greeks then...sailed away....

[The Horse is then dragged into the walled city of Troy and the people celebrate the end of the long war.]

...In the night, the armed men who were enclosed in the body of the horse...opened the gates of the city to their friends, who had returned under cover of the night. The city was set on fire; the people, overcome with feasting and sleep, put to the sword, and Troy completely subdued.

Bullfinch’s *Mythology* thus describes the original Trojan Horse. See <<http://homepage.mac.com/cparada/GML/WOODENHORSE.html>> for extensive information about the story. Today’s electronic Trojan is a program which conceals dangerous functions behind an outwardly innocuous form.

### 7.1 Case studies

One of the nastiest tricks played on the shell-shocked world of microcomputer users was the FLU-SHOT-4 incident of March 1988. With the publicity given to damage caused by destructive, self-replicating virus programs distributed through electronic bulletin board systems (BBS), it seemed natural that public-spirited programmers would rise to the challenge and provide protective screening.

- Flu-Shot-3 was a useful program for detecting viruses. Flu-Shot-4 appeared on BBS and looked just like 3; however, it actually destroyed critical areas of hard disks and any floppies present when the program was run. The instructions which caused the damage were not present in the program file until it was running; this self-modifying code technique makes it especially difficult to identify Trojans by simple inspection of the assembler-level code.
- HP itself put a Trojan into the HP3000 operating system with IOCDPN0.PUB.SYS. This program’s name implied that it ought to be an I/O driver for a CarD PuNch, just like IOTERM0 and IODISC0. Indeed, IOCDPN0 was tagged as a required driver by SYSDUMP so you couldn’t get rid of it. However, rather than being an innocuous old driver, the program was actually a powerful utility for accessing the low-level routine ATTACHIO. Using IOCDPN0, one could read and write to the memory structures controlling terminals, tapes, printers, and other peripherals. There were even macros to permit HP technicians to repeat I/O operations when MPE couldn’t help because of bad data or other unacceptable conditions. A typical use would be to read a bad tape and recover valuable data unreadable through normal I/O.
- Another Trojan was a blocking-factor program that one of my colleagues wrote. This vanilla program, derived from the Contributed Software Library (CSL) from INTEREX, the International Association of HP Computer Users, calculated optimum blocking factors admirably--but it posted an invisible timed terminal read at an undocumented but fixed period after initialization. If the user knew exactly what to type at exactly which time, he or she could obtain system manager (SM)status and all other capabilities for their user ID for that session. In a sense, this example also illustrates the concept of a back door.
- An incident that looked like a Trojan Horse occurred in 1983, when HP issued one of its periodic revisions of the MPE/V operating system. My operations team and I were just beginning our acceptance tests at 03:00, after production had completed and the operator had finished a full backup. We shut down the HP3000, switched disk packs to the test configuration, and began booting the system with the fresh Master Installation Tapes from HP. To our horror, we saw the message “WARNING: EXPERIMENTAL SOFTWARE PASS ‘9’” appear on our console, followed by the usual “DO NOT INTERRUPT WHILE BOOTING.” Even though we knew that the only risk was that we’d trash our test disk packs, the message

still shocked us. It turned out to be a only a harmless leftover from the Master Installation Tape quality assurance process.

- One of the participants in my Information Systems Security course reported a case of tampering on a UNISYS mainframe used in a military installation. A user was catching up on his work one evening when suddenly his display showed every single file in all of his disk directories being deleted one by one. Nothing he could do would stop the process, which went on for several minutes.

He reported the incident immediately to his superior officers. Panic ensued until midnight, when the it was found that a program called JOKE.RUN had been assigned to the function key. The program merely listed file names with "DELETING..." in front of each. No files had actually been deleted. Investigation found the programmer responsible; the joke had originally been directed at a fellow programmer, but the redefinition of the function key had accidentally found itself into the installation diskettes for a revision of the workstation software. It took additional hours to check every single workstation on the base looking for this joke. The programmer's career was not enhanced by this incident.

Some of the first PC Trojans included

- The Scrambler (also known as the KEYBGR Trojan), which pretends to be a keyboard driver (KEYBGR.COM) but actually makes a smiley face move randomly around the screen
- The 12-Tricks Trojan, which masquerades as CORETEST.COM, a program for testing the speed of a hard disk but actually causes 12 different kinds of damage (e.g., garbling printer output, slowing screen displays, and formatting the hard disk)
- The PC Cyborg Trojan (or "AIDS Trojan"), which claims to be an AIDS information program but actually encrypts all directory entries, fills up the entire C: disk, and simulates COMMAND.COM but produces an error message in response to nearly all commands.

## 7.2 1993-1994: Internet monitoring attacks

Trojan attacks on the Internet were discovered in late 1993. Full information about all such attacks is available on the World Wide Web site run by CIAC, the Computer Incident Advisory Capability of the U.S. Department of Energy < <http://ciac.llnl.gov/ciac/index.html> >. On February 3, 1994, CIAC issued Bulletin *E-09: Network Monitoring Attacks*. The Bulletin announced,

CIAC and other response teams have observed many compromised systems surreptitiously monitoring network traffic, obtaining username, password, host-name combinations (and potentially other sensitive information) as users connect to remote systems using telnet, rlogin, and ftp. This is for both local and wide area network connections. The intruders may (and presumably do) use this information to compromise new hosts and expand the scope of the attacks. Once system administrators discover a compromised host, they must presume monitoring of all network transactions from or to any host "visible" on the network for the duration of the compromise, and that intruders potentially possess any of the information so exposed. The attacks proceed as follows. The intruders gain unauthorized, privileged access to a host that supports a network interface capable of monitoring the network in "promiscuous mode," reading every packet on the network whether addressed to the host or not. They accomplish this by exploiting unpatched vulnerabilities or learning a username, password, host-name combination from the monitoring log of another compromised host. The intruders then install a network monitoring tool that captures and records the initial portion of all network traffic for ftp, telnet, and rlogin sessions. They typically also install "Trojan" programs for login, ps, and telnetd to support their unauthorized access and other clandestine activities.

System administrators must begin by determining if intruders have compromised their systems. The CERT Coordination Center has released a tool to detect network interface devices in promiscuous mode. Instructions for obtaining and using the tool appears later in this bulletin--the tool is available via anonymous ftp. If a site discovers that intruders have compromised their systems, the site must determine the extent of the attack and perform recovery as described below. System administrators must also prevent future attacks as described below.

CIAC works closely with CERT-CC, the Computer Emergency Response Team Coordination Center of the Software Engineering Institute at Carnegie Mellon University in Pittsburgh, PA. The instructions from CERT-CC included detailed instructions on verifying the authenticity of affected programs and instructions on removing the key vulnerabilities.

A few weeks later, CIAC issued Bulletin E-12, which warned ominously,

The number of Internet sites compromised by the ongoing series of network monitoring (sniffing) attacks continues to increase. The number of accounts compromised world-wide is now estimated to exceed 100,000. This series of attacks represents the most serious Internet threat in its history.

**IMPORTANT: THESE NETWORK MONITORS DO NOT SPECIFICALLY TARGET INFORMATION FROM UNIX SYSTEMS; ALL SYSTEMS SUPPORTING NETWORK LOGINS ARE POTENTIALLY VULNERABLE. IT IS IMPERATIVE THAT SITES ACT TO SECURE THEIR SYSTEMS.**

#### Attack Description

The attacks are based on network monitoring software, known as a “sniffer”, installed surreptitiously by intruders. The sniffer records the initial 128 bytes of each login, telnet, and FTP session seen on the local network segment, compromising ALL traffic to or from any machine on the segment as well as traffic passing through the segment being monitored. The captured data includes the name of the destination host, the username, and the password used. This information is written to a file and is later used by the intruders to gain access to other machines.

Finally, another CIAC alert (E-20, May 6, 1994) warned of “A Trojan-horse program, CD-IT.ZIP, masquerading as an improved driver for Chinon CD-ROM drives, [which] corrupts system files and the hard disk.” This program affects any MS-DOS system where it is executed.

### **7.3 Cases from the INFOSEC Year in Review Database<sup>2</sup>**

- 1997.04.29      The Department of Energy’s Computer Incident Advisory Capability (CIAC) warned users not to fall prey to the AOL4FREE.COM Trojan, which tries to erase files on hard drives when it is run. A couple of months later, the NCSA worked with AOL technical staff to issue a press release listing the many names of additional Trojans; these run as TSRs (Terminate - Stay Resident programs) and capture user IDs and passwords, then send them by e-mail to Bad People. Reminder: do NOT open binary attachments at all from people you don’t know; scan all attachments from people you do know with anti-virus and anti-Trojan programs before opening. (EDUPAGE)
- 1997-11-06      Viewers of pornographic pictures on the sexygirls.com site were in for a surprise when they got their next phone bills. Toronto victims who downloaded a “special viewer” were actually installing a Trojan program that silently disconnected their connection to their normal ISP and reconnected them (with the modem speaker turned off) to a number in Moldova in central Europe. The long-distance charges then ratcheted up until the user disconnected the session — sometimes hours later, even when the victims switched to other, perhaps less prurient, sites. The same fraud was reported in Feb in New York City, where a federal judge ordered the scam shut down. An interesting note is that AT&T staff spotted the scam because of unusually high volume of traffic to Moldova, not usually a destination for many US phone calls. In November, the FTC won \$2.74M from the bandits to refund to the cheated customers.

---

<sup>2</sup> Kabay, M. E. (2005). INFOSEC Year in Review. See < <http://www2.norwich.edu/mkabay/iyir> > for details and instructions on downloading this free database. PDF reports are also available for download.

- 1998-01-05 Jared Sandberg, writing in the Wall Street Journal, reported on widespread fraud directed against naïve AOL users using widely-distributed Trojan Horse programs (“proggies”) that allow them to steal passwords. Another favorite trick that fools gullible users is the old “We need your password” popup that claims to be from AOL administrators. AOL reminds everyone that no one from AOL will ever ask users for their passwords.
- 1999-01-29 Peter Neumann summarized a serious case of software contamination in RISKS 20.18: At least 52 computer systems downloaded a TCP wrapper program directly from a distribution site after the program had been contaminated with a Trojan horse early in the morning of 21 Jan 1999. The Trojan horse provided trapdoor access to each of the contaminated systems, and also sent e-mail identifying each system that had just been contaminated. The 52 primary sites were notified by the CERT at CMU after the problem had been detected and fixed. Secondary downloads may also have occurred.”
- 1999-05-28 Network Associates Inc. anti-virus labs warned of a new Trojan called BackDoor-G being sent around the Net as spam in May. Users were tricked into installing “screen savers” that were nothing of the sort. The Trojan resembled the previous year’s Back Orifice program in providing remote administration — and back doors for criminals to infiltrate a system. A variant called “Armageddon” appeared within days in France.
- 1999-06-11 The Worm.Explore.Zip (aka “Trojan Explore.Zip) worm appeared in June as an attachment to e-mail masquerading as an innocuous compressed WinZIP file. The executable file used the icon from WinZIP to fool people into double-clicking it, at which time it began destroying files on disk. Within a week of its discovery in Israel on the 6th of June the worm had spread to more than 12 countries. Network Associates reported that ~70% of its largest 500 corporate customers were infected. [Readers should remember that the larger the number of computers in a company, the more likely that at least one will be infected even when infection rates are low. If the probability of infecting one system is “p” and there are “n” targets in a group each of which can be infected independently, the likelihood of at least one infection in the group is  $P = \{1 - (1 - p)^n\}$  which rises rapidly as n increases.]
- 1999-09-20 A couple of new Y2K-related virus/worms packaged as Trojan Horses were discovered in September. One e-mail Trojan called “Y2Kcount.exe” claimed that its attachment was a Y2K-countdown clock; actually it also sent user IDs and passwords out into the Net by e-mail. Microsoft reported finding eight different versions of the e-mail in circulation on the Net. The other, named “W32/Fix2001” came as an attachment ostensibly from the system administrator and urged the victims to install the “fix” to prevent Internet problems around the Y2K transition. Actually, the virus/worm would replicate through attachments to all outbound e-mail messages from the infected system. [These malicious programs are called “virus/worms” because they integrate into the operating system (i.e., they are virus-like) but also replicate through networks via e-mail (i.e., they are worm-like).]
- 2000-01-03 Finjan Software Blocks Win32.Crypto the First Time: Finjan Software, Inc. announced that its proactive first-strike security solution, SurfinShield Corporate, blocks the new Win32.Crypto malicious code attack. Win32.Crypto, a Trojan executable program released in the wild today, is unique in that infected computers become dependant on the Trojan as a “middle-man” in the operating system. Any attempt to disinfect it will result in the collapse of the operating system itself. It is a new kind of attack with particularly damaging consequences because attempting to remove the infection may render the computer useless and force a user to rebuild their system from scratch.
- 2000-08-29 Software companies . . . reported that the first . . . [malware] to target the Palm operating system has been discovered. The bug, which uses a “Trojan horse” strategy to infect its victims, comes disguised as pirated software purported to emulate a Nintendo Gameboy on Palm PDAs and then proceeds to delete applications on the device. The . . . [malware] does not pose a significant threat

to most users, says Gene Hodges, president of Network Associates' McAfee division, but signals a new era in technological vulnerability: "This is the beginning of yet another phase in the war against hackers and virus writers. In fact, the real significance of this latest Trojan discovery is the proof of concept that it represents." (Agence France Presse/New York Times 29 Aug 2000)

- 2000-10-27 Microsoft's internal computer network was invaded by the QAZ "Trojan horse" software that caused company passwords to be sent to an e-mail address in St. Petersburg, Russia. Calling the act "a deplorable act of industrial espionage," Microsoft would not say whether or not the hackers may have gotten hold of any Microsoft source code. (AP/New York Times 27 Oct 2000)
- However, within a few days, Microsoft . . . [said] that network vandals were able to invade the company's internal network for only 12 days (rather than 5 weeks, as it had originally reported), and that no major corporate secrets were stolen. Microsoft executive Rick Miller said: "We started seeing these new accounts being created, but that could be an anomaly of the system. After a day, we realized it was someone hacking into the system." At that point Microsoft began monitoring the illegal break-in, and reported it to the FBI. Miller said that, because of the immense size of the source code files, it was unlikely that the invaders would have been able to copy them. (AP/Washington Post 30 Oct 2000)
- 2002-01-19 A patch for a vulnerability in the AOL Instant Messenger (AIM) program was converted into a Trojan horse that initiated unauthorized click-throughs on advertising icons, divulged system information to third parties and browsed to porn sites.
- 2002-03-11 The "Gibe" worm was circulated in March 2002 as a 160KB EXE file attached to a cover message pretending to be a Microsoft alert explaining that the file was a "cumulative patch" and pointing vaguely to a Microsoft security site. Going to the site showed no sign of any such patch, nor was there a digital signature for the file. However, naive recipients were susceptible to the trick.
- [MORAL: keep warning recipients not to open unsolicited attachments in e-mail.]
- 2002-04-03 Nicholas C. Weaver warned in RISKS that the company Brilliant Digital (BD) formally announced distribution of Trojan software via the Kazaa peer-to-peer network software. The BD software would create a P2P server network to be used for distributed storage, computation and communication -- all of which would pose serious security risks to everyone concerned. Weaver pointed out that today's naïve users appear to be ready to agree to anything at all that is included in a license agreement, whether it is in their interests or not.
- 2003-02-14 E-mail purporting to offer revealing photos of Catherine Zeta-Jones, Britney Spears, and other celebrities is actually offering something quite different: the secret installation of Trojan horse software that can be used by intruders to take over your computer. Users of the Kazaa file-sharing service and IRC instant messaging are at risk. (Reuters/USA Today 14 Feb 2003)
- 2003-05-22 Data security software developer Kaspersky Labs reports that a new Trojan program, StartPage, is exploiting an Internet Explorer vulnerability for which there is no patch. If a patch is not released soon, other viruses could exploit the vulnerability. StartPage is sent to victim addresses directly from the author and does not have an automatic send function. The program is a Zip-archive that contains an HTML file. Upon opening the HTML file, an embedded Java-script is launched that exploits the "Exploit.SelfExecHtml" vulnerability and clandestinely executes an embedded EXE file carrying the Trojan program.
- 2003-07-14 Close to 2,000 Windows-based PCs with high-speed Internet connections have been hijacked by a stealth program and are being used to send ads for pornography, computer security experts warned. It is unknown exactly how the trojan (dubbed "Migmaf" for "migrant Mafia") is spreading to victim computers around the world, whose owners most likely have no idea what is happening, said Richard M. Smith, a security consultant in Boston. The trojan turns the victim

computer into a proxy server which serves as a middle man between people clicking on porn e-mail spam or Web site links, according to Smith. The victim computer acts as a “front” to the porn Web site, enabling the porn Web servers to hide their location, Smith said. Broadband Internet users should always use firewalls to block such stealth activity, he said. Computers with updated anti-virus software will also be protected, said Lisa Smith of network security company Network Associate’s.

- 2004-01-08 BackDoor-AWQ.b is a remote access Trojan written in Borland Delphi, according to McAfee, which issued an alert Tuesday, January 6. An email message constructed to download and execute the Trojan is known to have been spammed to users. The spammed message is constructed in HTML format. It is likely to have a random subject line, and its body is likely to bear a head portrait of a lady (loaded from a remote server upon viewing the message). The body contains HTML tags to load a second file from a remote server. This file is MIME, and contains the remote access Trojan (base64 encoded). Upon execution, the Trojan installs itself into the %SysDir% directory as GRAYPIGEON.EXE. A DLL file is extracted and also copied to this directory (where %Sysdir% is the Windows System directory, for example C:\WINNT\SYSTEM32) The following Registry key is added to hook system startup: HKEY\_CURRENT\_USER\Software\Microsoft\Windows\CurrentVersion \RunOnce “ScanRegedit” = “%SysDir%\GRAYPIGEON.EXE” The DLL file (which contains the backdoor functionality) is injected into the EXPLORER.EXE process on the victim machine. More information, including removal instructions, can be found at: [http://us.mcafee.com/virusInfo/default.asp?id=description &virus\\_k=100938](http://us.mcafee.com/virusInfo/default.asp?id=description &virus_k=100938)
- 2004-01-09 A Trojan horse program that appears to be a Microsoft Corp. security update can download malicious code from a remote Web site and install a back door on the compromised computer, leaving it vulnerable to remote control. Idefense Inc., a Reston, Va., computer security company, said the malicious code is the latest example of so-called social engineering to fool Windows users. It is similar to the W32Sven worm, which last year passed itself off as a Microsoft patch.
- 2004-03-17 The U.S. Department of Homeland Security has alerted computer security experts about the Phatbot Trojan, which snoops for passwords on infected computers and tries to disable firewall and antivirus software. Phatbot . . . Has proved difficult for law enforcement authorities and antivirus companies to fight.... Mikko Hypponen, director of the antivirus software company F-Secure in Finland says, “With these P2P Trojan networks, even if you take down half of the affected machines, the rest of the network continues to work just fine”; security expert Russ Cooper of TruSecure warns, “If there are indeed hundreds of thousands of computers infected with Phatbot, U.S. e-commerce is in serious threat of being massively attacked by whoever owns these networks.” (Washington Post 17 Mar 2004)
- 2004-05-12 Intego has identified a Trojan horse — AS.MW2004.Trojan — that affects Mac OS X. This Trojan horse, when double-clicked, permanently deletes all the files in the current user’s home folder. Intego has notified Apple, Microsoft and the CERT, and has been working in close collaboration with these companies and organizations. The AS.MW2004.Trojan is a compiled AppleScript applet, a 108 KB self-contained application, with an icon resembling an installer for Microsoft Office 2004 for Mac OS X. This AppleScript runs a Unix command that removes files, using AppleScript’s ability to run such commands. The AppleScript displays no messages, dialogs or alerts. Once the user double-clicks this file, their home folder and all its contents are deleted permanently. All Macintosh users should only download and run applications from trusted sources.
- 2004-05-18 Security experts are tracking two new threats that have emerged in the past few days, including a worm that uses seven mechanisms to spread itself. The worm is known as Kibuv, and researchers first noticed its presence Friday, May 14. Kibuv affects all versions of Windows from 98 through Windows Server 2003 and attempts to spread through a variety of methods, including exploiting five Windows vulnerabilities and connecting to the FTP server installed by the Sasser worms. The

worm has not spread too widely as of yet, but with its variety of infection methods, experts say the potential exists for it to infect a large number of machines. The second piece of malware that has surfaced is a Trojan that is capable of spreading semi-automatically. Known as Bobax, the Trojan can only infect machines running Windows XP and seems to exist solely for the purpose of sending out large amounts of spam. When ordered to scan for new machines to infect, Bobax spawns 128 threads and begins scanning for PCs with TCP port 5000 open. If the port is open, it exploits the Windows LSASS vulnerability. Bobax then loads a copy of itself onto the new PC, and the process repeats. Antivirus and antis spam providers say they have seen just a few machines infected with Bobax as of Tuesday, May 18.

- 2004-05-20 A Trojan horse may be responsible for an online banking scam that has cost at least two Winnipeg, Canada, customers thousands of dollars. The Winnipeg Police Service is investigating two cases where money was transferred unknowingly from bank accounts. The investigation is focused around a man who recently emigrated to Canada from an unidentified locale in Eastern Europe. According to computer security experts, online banking scams and identity theft are proliferating in Canada. While Canadian e-banking customers have yet to see a surge in identity theft similar to the U.S., the banks say the onus is on consumers and enterprises to protect themselves. Keystroke loggers are the most frequently used tactic for crooks targeting banking information, said Tom Slodichak, chief security officer of WhiteHat, an IT security provider. "Although a Web session with their financial institution is usually encrypted, the keystroke logger intercepts the keystrokes before any encryption occurs, so they will get all the information—the account numbers, the names, the passwords or PINs or whatever they need to impersonate that [individual]," he said.
- 2004-08-10 Malicious code that dials premium rate numbers without a user's consent has been found in a pirated version of Mosquitos 2.0, a popular game for Symbian Series 60 smartphones. The illicit copies of the game are circulating over P2P networks. News of the Symbian Trojan dialler comes days after the arrival of the first Trojan for handheld computers running Windows Pocket PC operating system, Brador-A.
- 2004-10-25 An e-mail disguised as a Red Hat patch update is a fake designed to trick users into downloading malware designed to compromise the systems they run on, the Linux vendor warned in a message on its Website. While the malicious site was taken down over the weekend, the SANS Internet Storm Center posted a message on its Website saying the hoax "is a good reminder that even though most of these are aimed at Windows users, always be suspect when receiving an e-mail asking you to download something."
- 2004-11-23 A new attack by Trojan Horse software known as "Skulls" targets Nokia 7610 cell phones, rendering infected handsets almost useless. The program appears to be a "theme manager" for the phone. It replaces most of an infected phone's program icons with images of skulls and crossbones, and disables all of the default programs on the phone (calendar, phonebook, camera, Web browser, SMS applications, etc.) -- i.e., essentially everything except normal phone calls. Symbian, the maker of the Nokia 7610 operating system, says that users will only be affected if they knowingly and deliberately install the file and ignore the warnings that the phone displays at the conclusion of the installation process. Experts don't consider the Skulls malware to be a major threat, but note that it's the third mobile phone bug to appear this year -- and therefore probably means that this kind of problem is here for the foreseeable future. (ENN Electronic News.net 23 Nov 2004)
- 2005-01-13 Users are being warned about the Cellery worm -- a Windows virus that piggybacks on the hugely popular Tetris game. Rather than spreading itself via e-mail, Cellery installs a playable version of Tetris on the user's machine. When the game starts up, the worm seeks out other computers it can infect on the same network. The virus does no damage, but could result in clogged traffic on heavily infected networks. "If your company has a culture of allowing games to be played in the office, your staff may believe this is simply a new game that has been installed -- rather than

something that should cause concern,” says a spokesman for computer security firm Sophos. (BBC News 13 Jan 2005)

2005-01-24 Two new Trojan horse programs, Gavno.a and Gavno.b, masquerade as patch files designed to trick users into downloading them, says Aaron Davidson, chief executive officer of SimWorks International. Although almost identical with Gavno.a, Gavno.b contains the Cabir worm, which attempts to send a copy of the Trojan horse to other nearby Symbian-based phones via short-range wireless Bluetooth technology. The Gavno Trojans, according to Davidson, are the first to aim at disrupting a core function of mobile phones—telephony—in addition to other applications such as text messaging, e-mail, and address books. Gavno.a and Gavno.b are proof-of-concept Trojan horses that “are not yet in the wild,” Davidson says. Davidson believes the Trojan programs originated in Russia. To fix infected phones, users will need to restore them to their factory settings.

2005-02-11 Microsoft Corp is investigating a malicious program that attempts to turn off the company’s newly released anti-spyware software for Windows computers. Stephen Toulouse, a Microsoft security program manager, said yesterday that the program, known as “Bankash-A Trojan,” could attempt to disable or delete the spyware removal tool and suppress warning messages. It also may try to steal online banking passwords or other personal information by tracking a user’s keystrokes. To be attacked, Toulouse said a user would have to be fooled into opening an email attachment that would then start the malicious program. (The Age 11 Feb 2005)

SOPHOS anti-malware company summarizes the Trojan’s functions as follows:

- \* Steals credit card details
- \* Turns off anti-virus applications
- \* Deletes files off the computer
- \* Steals information
- \* Drops more malware
- \* Downloads code from the internet

2005-04-08 On Thursday, April 7, the same day that Microsoft announced details of its next round of monthly patches, hackers sent out a wave of emails disguised as messages from the software company in a bid to take control of thousands of computers. The emails contain bogus news of a Microsoft update, advising people to open a link to a Web site and download a file that will secure and ‘patch’ their PCs. The fake Website, which is hosted in Australia, looks almost identical to Microsoft’s and the download is actually a Trojan horse — a program that can give hackers remote control of a computer. Microsoft said it is looking into the situation.

## **7.4 Hardware Trojans**

On November 8, 1994, a correspondent reported to the RISKS Forum Digest that he had been victimized by a curious kind of Trojan:

I recently purchased an Apple Macintosh computer at a “computer superstore,” as separate components - the Apple CPU, and Apple monitor, and a third-party keyboard billed as coming from a company called Sicon.

This past weekend, while trying to get some text-editing work done, I had to leave the computer alone for a while. Upon returning, I found to my horror that the text “welcome datacomp” had been \*inserted into the text I was editing\*. I was certain that I hadn’t typed it, and my wife verified that she hadn’t, either. A quick survey showed that the “clipboard” (the repository for information being manipulated via cut/paste operations) wasn’t the source of the offending text.

As usual, the initial reaction was to suspect a virus. Disinfectant, a leading anti-viral application for Macintoshes, gave the system a clean bill of health; furthermore, its descriptions of the known viruses (as of Disinfectant version 3.5, the latest release) did not mention any symptoms similar to my experiences.



I restarted the system in a fully minimal configuration, launched an editor, and waited. Sure enough, after a (rather long) wait, the text “welcome datacomp” once again appeared, all at once, on its own.

Further investigation revealed that someone had put unauthorized code in the ROM chip used in several brands of keyboard. The only solution was to replace the keyboard. Readers will understand the possible consequences of a keyboard which inserts unauthorized text into, say, source code. Winn Schwartau has coined the word, “chipping” to refer to such unauthorized modification of firmware.<sup>3</sup>

## **7.5 Diagnosis and prevention**

It is difficult to identify Trojans because, like the ancient Horse built by the Greeks, they don’t reveal their nature immediately. The first step in catching a Trojan is to run the program on an isolated system. That is, try the candidate either on a system whose hard disk drives have been disconnected or which is reserved exclusively for testing new programs.

While the program is executing, look for unexpected disk drive activity; if your drives have separate read/write indicators, check for write activity on drives.

Some Trojans running on micro-computers use unusual methods of accessing disks; various products exist which trap such programmatic devices. Such products, aimed mostly at interfering with viruses, usually interrupt execution of unusual or suspect instructions and indicate what’s happening but prevent the damage from occurring. Several products can “learn” about legitimate events used by proven programs and thus adapt to your own particular environment.

If the Trojan is a replacement for specific components of the operating system, as in the network monitoring problem described by CIAC above, it is possible to compute check sums and compare them with published checksums for the authentic modules.

The ideal situation for a microcomputer user or a system/network manager is to know, for every executable file (e.g., PROG, .COM, or .EXE) on the system

- Where it comes from
- What it’s supposed to do.

Take, for example, shareware programs. In general, each program should come not only with the name and address of the person submitting it for distribution but also with the source code. If the requisite compiler is available, one can even compare the object code available on the tape or diskette with the results of a fresh compilation and linkage to be sure there are no discrepancies. These measures make it easier to hope for Trojan-free utilities.

It makes sense for system managers to forbid the introduction of foreign software into their systems and networks without adequate testing. Users wishing to install apparently useful utilities should contact their system support staff to arrange for acceptance tests. Installing software of unknown quality on a production system is irresponsible.

When organizations develop their own software, the best protection against Trojans is quality assurance and testing (QAT). QAT should be carried out by someone other than the programmer(s) who created the program being tested. QAT procedures often include structured walk-throughs, in which designers are asked to explain every section of their proposed system. In later phases, programmers have to explain their code to the QAT team. During systems tests, QAT specialists have to ensure that every line of source code is actually executed at least once. Under these circumstances, it is difficult to conceal unauthorized functions in a Trojan.

---

<sup>3</sup> Tate, C. (1994). Hardware-borne Trojan Horse programs. RISKS 16.55 < <http://catless.newcastle.ac.uk/Risks/16.55.html#subj3> >

## 8 Back Doors: Secret Access

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.

### 8.1 Origins

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.

### 8.2 Examples of Back Doors

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.

### **8.3 Easter Eggs and the Trusted Computing Base**

In March 2000, I spoke at NATO headquarters in Brussels in an unclassified security-awareness briefing concerning computer crime implications for national security. The following is a summary of part of my presentation there.

The confluence of several security threats has destroyed the Trusted Computing Base (TCB) on which security has depended for the last two decades.

The TCB was the constellation of trustworthy hardware, operating system, and application software that allowed for predictable results from predictable inputs.

- Did you know that there is a flight simulator concealed in MS-Excel 97? To access this game, you use the following sequence of commands (detailed by Larry Werring in RISKS DIGEST 19.53 on 19998-01-05):
- Open Excel 97.
- Open a new worksheet and press the F5 key.
- Type X97:L97 and press the Enter key.
- Press the Tab key.
- Hold Ctrl-Shift and click the Chart Wizard button on the tool bar.
- Once the Easter egg is activated, use the mouse to fly around – right button for forward, left for reverse.

If you have DirectX drivers installed, a bizarre landscape appears and you can “fly” over (or under) the geometric forms by using the arrow keys on your keyboard. If you look carefully in the virtual distance, you can find a stone monitor planted in the ground. If you get close enough, you can see the names of the development team scrolling by.

How much space in the source and object code does this Easter Egg take? How much RAM and disk space are being wasted in total by all the people who have installed and are using this product? And much more seriously, what does this Easter Egg imply about the quality assurance at the manufacturer’s offices?

An Easter Egg is presumably undocumented code – or at least, it’s undocumented for the users. I do not know if it is documented in internal Microsoft documents. However, I think that the fact that this undocumented function got through Microsoft’s quality assurance process is terribly significant. I think that the failure implies that there is no test-coverage monitoring in that QA process.

When testing executables, one of the necessary (but not sufficient) tests is coverage: how much of the executable code has actually been executed at least once during the QA process. Without running all the code at least once, one can state with certainty that the test process is incomplete. Failing to execute all the code means that there may be hidden functionality in the program: anything from an Easter Egg to something worse. What if the undiscovered code were to be invoked in unusual circumstances and cause damage to a user’s spreadsheet or system? We would call such code a logic bomb.

That’s bad enough, but it gets worse. Consider the following observations:

- There is already at least one family of Excel macro virus that alters the contents of cells; the Macro.Excel.Sugar virus randomly inserts silly text into up to 200 cells. This payload is immediately obvious, but more insidious Excel macro viruses might cause subtle problems. For example, a virus could cause shifts in the low-order significant digits of constants – something that might not be noticed in individual cells but which might have significant effects on calculated results.
- Research projects 1997 by Coopers & Lybrand in London, England showed that 90% of all the spreadsheets with more than 150 rows had errors in them; research on production spreadsheets by University of Hawaii scientists revealed that in 300 files tested and in experiments with more than 1000 users, many spreadsheets contained at least one significant formula mistake.
- In December 1999, Computer Associates issued a warning about the W.95.Babylonia virus, described as an extensible virus whose payload could be modified remotely by its author. The December outbreak of Babylonia in the wild involved a Trojan disguised as a Y2K bug fix for Internet Relay Chat (IRC) users. The Trojan would send itself to other users and also poll an Internet site in Japan looking for updated plugins to alter the effects of the malicious software.
- Distributed computing in today’s Internet means that most naive users accepted code from Web sites with little awareness of the dangers of executing unknown and perhaps poorly tested or frankly malicious code on their desktop.
- Recent distributed denial-of-service attacks have shown how easy it is to install unauthorized code on Internet-connected systems and have that code lie quiescent until instructions are broadcast from a master program on a remote system.

Well then, here’s the scenario: Bad Guys infiltrate major software company and install undocumented code in widely-distributed spreadsheet software. Faulty quality assurance allows the logic bomb to go into production releases.

The logic bomb in the spreadsheet software receives payload instructions from an Internet connection.

At a specified time, the spreadsheet program alters data in millions of spreadsheets in, say, the USA. Calculations go awry in subtle but dangerous ways. Since almost no one bothers to document their spreadsheets or provide test suites that can validate the calculations, few people notice the changes. Business, engineering, medical, and academic users make mistakes – they allocate the wrong amounts to investments and inventory, they predict the wrong stresses on bridge components, they calculate bad dosages for patient medication, and they assign good grades to bad students.

This situation leads to decreased efficiency in the US economy and is a contributing factor to a national and eventually international recession.

This scenario is an example of asymmetric information warfare – electronic sabotage on a grand scale but for low cost. Winn Schwartau used just this kind of scenario in his 1991 novel, *Terminal Compromise* – great fun and available online free < <http://ftp.archive.org/etext/etext93/termc10.txt> > or as a printed book (ASIN 0962870005).

So the next time you play with an Easter Egg in commercial software, stop to think: shouldn't you express your concerns to the manufacturer instead of just chuckling over a programmer's joke?

## 8.4 Back Doors: RATs

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 LOPHT 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 listed in the references at the end of this paper.

## **8.5 Back Doors: Testing Source Code**

In this section, 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 addition to the Excel 97 flight simulator mentioned earlier (see < <http://www.eeggs.com/items/29841.html> >), you can activate a spy hunter game that uses DirectX for graphics in Excel 2000 (see < <http://www.eeggs.com/items/8240.html> >).

## 8.6 Additional resources

Diane Levine's chapter on software development and quality assurance in the *Computer Security Handbook*, 4<sup>th</sup> edition is an excellent primer on how quality assurance is fundamental to security and will be studied later in the MSIA program.

- 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.html> > with short descriptions of each tool and pointers to where they can be obtained.

## 8.7 Additional reports

The IYIR<sup>4</sup> has a section reserved for remote-control issues, including remote reprogramming as a design feature of safety-critical systems. Here's a list of some of the items:

- 1997-08-21      MediVIEW and Medically Oriented Operating Network (MOON) from Sabratek Corp. allow intensive remote medical intervention such as alterations of automated flow control devices for drug administration. The initial press releases included no sign that anyone was concerned about security issues in this system. [The risks of system error and hacking now become life-threatening.]
- 1999-07-12      David Hellaby of the Canberra Times (Australia) published a good review of remote-control software used by criminal hackers. Some of the dangerous applications are BackOrifice, BackOrifice 2000, DeepThroat 1, 2 and 3, EvilFTP, ExploreZip.worm, GateCrasher 1.2, GirlFriend 1.3, Hack'a'Tack, NetSphere 1.30, phAse Zero, Portal of Doom, and SubSeven (aka BackDoor-G). These programs are usually integrated into otherwise harmless and useful vector programs to create Trojans that are downloaded from the Net or shared among hapless victims. Symptoms of remote control sound like a nightmare from a paranoid schizophrenic's worst crisis: "your CD draw begins opening and closing, your web browser starts on its own, strange messages appear on your screen, and your PC seems to be haunted." The author warned his readers to be very careful about opening attachments to e-mail messages.
- 2000-05-31      The General Motors OnStar system will allow not only geographical positioning data, local information, and outbound signaling in case of accidents: it will also allow inbound remote control of features such as door locks, headlights, the horn and so on — all presumably useful in emergencies. However, Armando Fox commented in RISKS, >If I were a cell phone data services hacker, I'd know what my next project would be. I asked the OnStar speaker what security mechanisms were in place to prevent your car being hacked. He assured me that the mechanisms in place were "very secure". I asked whether he could describe them, but he could not because they were also "very proprietary". \*Sigh\*<

---

<sup>4</sup> Kabay, M. E. (2005). INFOSEC Year in Review. See < <http://www2.norwich.edu/mkabay/iyr> > for details and instructions on downloading this free database. PDF reports are also available for download.

- 2000-08-17 Anatole Shaw reported in RISKS on a dreadful new development in mobile attack weapons: “The Thailand Research Fund has unveiled a new robot, resembling a giant ladybug with a couple of extra limbs. The unit is equipped with visible-spectrum and thermal vision, and a gun. According to Prof. Pitikhet Suraksa, its shooting habits can be automated, or controlled ‘from anywhere through the Internet’ with a password. The risks of both modes are obvious, but the latter is new to this arena. Police robots of this ilk have been around for a long time, but are generally radio-controlled. The apparent goal here is to make remote firepower available on-the-spot from around the Internet, which means insecure clients everywhere. How long will it take for one of these passwords to be leaked via a keyboard capture, or a browser bug? Slowly, we’re bringing the risks of online banking to projectile weaponry.”
- 2000-08-25 Several hundred users of new Japanese programmable wireless phones were harassed when someone remotely ordered their devices to dial the emergency services. Kevin Connolly commented in RISKS, “The risk is that people designing new mobile phone functions do not learn from the mistakes in the MS Word macro ‘virus enabling’ feature.”
- 2000-10-20 A gateway sold by National Instruments allows instruments equipped with the standard IEEE-488 bus to be connected to the Internet — completely without any security provisions — and thus controlled remotely by total strangers. The usual dangers to the electronic equipment are exacerbated, wrote Stephen D. Holland in RISKS, because laboratory equipment is often used to control mechanical devices.
- 2000-12-22 In the early 1990s, certain tape drives were criticized for allowing uncontrollable automatic firmware upgrades if a “firmware-configuration tape” was recognized. The problems occurred when the tape drive “recognized” a tape as such even if it wasn’t. A decade later, the same type of feature — and problem — has been noted in Dolby digital sound processors for the audio tracks of 35mm film: any time anything looking like a firmware-reconfiguration data stream is encountered, the device attempts to reconfigure itself, regardless of validity of the data stream or the wishes of the operator. A German contributor to a discussion group about movie projectors noted (translation by Marc Roessler), “The trailer of “Billy Elliott” has got some nasty bug: If the trailer is being cut right behind start mark three, the CP500 will do a software reset with data upload as the trailer runs through the machine. Either Dolby Digital crashes completely or the Cat 673 is set to factory default, which means setting the digital soundhead delay to 500 perforations, i.e. the digital sound lags 5.5 seconds behind the picture. . . .”
- 2000-12-27 Andrew Klossner noted in RISKS that home electronics such as DVDs are being reprogrammed using automatic firmware upgrades from media (e.g., DVDs). The correspondent writes, “When the authoritarian software forbids me to skip past a twenty-second copyright notice, it makes me nostalgic for the old 12-inch laser disks.” [MK notes: This poses additional sources of troublesome problems when the software doesn’t work right. Even if it isn’t broke, someone at a distance may try to fix it anyway.]
- 2001-01-12 Daniel P. B. Smith reported in RISKS that a new airborne laser is being designed to shoot down missiles. Smith quotes an article at <<http://www.cnn.com/2001/US/01/12/airborne.laser/index.html>> as follows: >No trigger man. No human finger will actually pull a trigger. Onboard computers will decide when to fire the beam. Machinery will be programmed to fire because human beings may not be fast enough to determine whether a situation warrants the laser’s use, said Col. Lynn Wills of U.S. Air Force Air Combat Command, who is to oversee the battle management suite. The nose-cone turret is still under construction. “This all has to happen much too fast,” Wills said. “We will give the computer its rules of engagement before the mission, and it will have orders to fire when the conditions call for it.” The laser has about only an 18-second “kill window” in which to lock on and destroy a rising missile, said Wills. “We not only have to be fast, we have to be very careful about where we shoot,” said Wills, who noted that the firing system will have a manual override. “The last thing we want to do is lase an F-22 (fighter jet).” [MK: Readers are invited to decide if, given the



current state of software quality assurance worldwide, they would be willing to entrust the safety of their family to an automobile equipped with analogous control systems.]

- 2001-01-19 Steve Loughran noted in RISKS that the British government has sponsored tests of computer-controlled speed governors for automobiles; the system would rely on a GPS to locate the vehicle and an on-board database of speed limits. Loughran commented, "Just think how much fun you'll be able to have by a UK motorway in five years time from jamming the GPS signals. Or how much a 'chipped' database or speed limiter will be worth. A more rigorous trial would be to place the speed limited vehicles in the hands of well known violators of the speed laws to see how much effort it takes to disable -- the UK home secretary himself, for example." In addition, the prospect of being unable to take evasive action in an emergency should cause grave concern. Furthermore, given the dismal state of software quality assurance, few RISKS readers would be happy with such a system.
- 2001-01-26 Jeremy Epstein wrote an interesting report for RISKS on remote reprogramming: "DirectTV has the capability to remotely reprogram the smart cards used to access their service, and also to reprogram the settop box. To make a long story short, they were able to trick hackers into accepting updates to the smart cards a few bytes at a time. Once a complete update was installed on the smart cards, they sent out a command that caused all counterfeit cards to go into an infinite loop, thus rendering them useless."
- 2001-03-30 Microsoft Networks (MSN) upgraded its dialup lists automatically for users in the Research Triangle, NC area -- and wiped out several local access node numbers. Outraged users found out (too late) that their modems had switched to dialing access nodes in areas reached through long distance calls. About a month later, MSN reimbursed its customers for the long-distance calls their modems had placed due to MSN's errors.
- 2001-04-09 Appliance hacking has been a subject of speculation for years, but more and more manufacturers are interested in controlling their domestic appliances at a distance. According to a report in RISKS, "IBM and Carrier, an air-conditioning manufacturer, said they plan to offer Web-enabled air conditioners in Europe this summer that can be controlled wirelessly. Financial terms of the collaboration were not disclosed. Owners of the newfangled air conditioners will be able to set temperatures or switch the units on or off wirelessly using a website called Myappliance.com < <http://www.wired.com/news/business/0,1367,42918,00.html> >. The press release quoted in RISKS indicates that the system will log information about device utilization and allow remote maintenance operations.
- 2001-04-10 IBM and the Carrier Corp., which makes heating and air conditioning systems, is planning a pilot program this summer in Britain, Greece and Italy to test an Internet-based system that would allow people to use a Web site, myappliance.com, to control their home air conditioners from work or elsewhere. The system will allow troubleshooting to be done remotely and will make it easier to conserve electricity during peak demand periods. (AP/New York Times 9 Apr 2001)
- 2001-09-06 A new Web-based service called GoToMyPC enables users to control their desktop PCs in their homes or offices using any other Windows PC anywhere in the world that has Internet access. The service, a brainchild of Expertcity Inc., costs \$10 a month. Instead of lugging a laptop along on a trip, a user could sit down at an Internet café PC and access all files, e-mail, etc. on his or her PC at home. Alternatively, if a worker found that the file he or she needed over the weekend was on the computer at work, it could be retrieved using the service. The company says the system is highly secure and requires two passwords -- one to log onto the service and another to gain access to each target PC. All of the data exchanged in each remote-control session is encrypted and Expertcity says the service will operate through many corporate firewalls. (Wall Street Journal 6 Sep 2001)

- 2001-10-01 Steve Bellovin contributed an item to RISKS about remote control of airplanes: "The Associated Press reported on a test of a remotely-piloted 727. The utility of such a scheme is clear, in the wake of the recent attacks; to the reporter's credit, the article spent most of its space discussing whether or not this would actually be an improvement. The major focus of the doubters was on security: But other experts suggested privately that they would be more concerned about terrorists' ability to gain control of planes from the ground than to hijack them in the air. I'm sure RISKS readers can think of many other concerns, including the accuracy of the GPS system the tested scheme used for navigation (the vulnerabilities of GPS were discussed recently in RISKS), and the reliability of the computer programs that would manage such remote control."
- 2001-12-20 In a discussion of "the telesurgery revolution" in *The Futurist* magazine, surgeon Jacques Marescau, a professor at the European Institute of Telesurgery, offers the following description of the success of the remotely performed surgical procedure as the beginning of a "third revolution" in surgery within the last decade: "The first was the arrival of minimally invasive surgery, enabling procedures to be performed with guidance by a camera, meaning that the abdomen and thorax do not have to be opened. The second was the introduction of computer-assisted surgery, where sophisticated software algorithms enhance the safety of the surgeon's movements during a procedure, rendering them more accurate, while introducing the concept of distance between the surgeon and the patient. It was thus a natural extrapolation to imagine that this distance--currently several meters in the operating room--could potentially be up to several thousand kilometers." A high-speed fiber optic connection between New York and France makes it possible to achieve an average time delay of only 150 milliseconds. "I felt as comfortable operating on my patient as if I had been in the room," says Marescaux. (*The Futurist* Jan/Feb 2002)
- 2002-01-08 J. P. Gilliver noted an alarming development in remote reprogramming -- an easy way to modify firmware: ". . . For example, IRL (Internet Reconfigurable Logic) means that a new design can be sent to an FPGA in any system based on its IP address." (From Robert Green, Strategic Solutions Marketing with Xilinx Ltd., in "Electronic Product Design" December 2001. Xilinx is a big manufacturer of FPGAs.) For those unfamiliar with the term, FPGA stands for field-programmable logic array: many modern designs are built using these devices, which replace tens or hundreds of thousands of gates of hard-wired logic. The RISKS involved are left as an exercise to the readers."
- 2002-01-16 Researchers at the University of California in San Diego have developed a way to blow up silicon chips using an electric signal -- an innovation that could be used to fry electronic circuitry in devices after they're stolen or fall into the wrong hands. The American spy plane that was impounded in China last year is an example where such technology would have proven handy in destroying its secret electronics systems. Similarly, if a cell phone were stolen, the owner could alert the wireless carrier, which would send a signal to trigger a small explosion in the phone's chip, rendering it useless. The techniques uses a small amount of the oxidizing chemical gadolinium nitrate applied to a porous silicon wafer. (*New Scientist* 16 Jan 2002)
- 2002-01-25 In Switzerland, the mobile phone company Swisscom admitted that it reconfigured its customers' phones using a program embedded in a SMS (short message service) transmission. The message deleted roaming information. S. Llabres reported in RISKS, ". . . [I]nsiders believe that the modification of the roaming information was to direct traffic to networks owned by Vodafone -- which acquired a 25% share of Swisscom [in April] last year." Llabres commented astutely, "It would be interesting:  
\* If there is any security mechanism protecting anyone from sending such "special" messages.  
\* Which setting[s] on the mobile phone can be changed (or probably retrieved from the phone) without knowledge to the customer.  
\* If the network provider must implement such features, I do not understand why this must happen unperceived by the customer. Why not send a message telling people what will happen?"

- 2002-02-20 Scott Schram published a paper at < <http://schram.net/articles/updaterisk.html> > that pointed out the security risks of all auto-update programs (e.g., self-updating antivirus products, MS Internet Explorer, MS-Windows Update, and so on). Once the firewall has been set to trust their activity, there is absolutely no further control possible over what these programs do. If any of them should ever be compromised, the results on trusting systems would be potentially catastrophic.
- 2002-03-14 In March 2002, tests on unmanned remote-control aircraft studied the effectiveness of automated collision-avoidance systems. Look for exciting developments in security-engineering failures in years to come.
- 2002-03-18 In Boston, city engineers described plans for a new highway-traffic monitoring system called the Integrated Project Control System (IPCS). Using magnetic loops embedded in the pavement, the system would sense traffic speed and instantly report sudden slowdowns or stoppages as well as simply keeping track of total volume and speed for statistical purposes.
- 2002-04-22 John McPherson noted in RISKS: "... The Matamata wireless link replaced an expensive frame relay service as well as providing a 1Mbs Internet service to several outlying sites including a library and remote management of water supplies. As the water facilities are computer controlled, they are able to manipulate them remotely rather than sending someone 20 miles down the road just to turn a valve." ... From \*The New Zealand Herald\* (Talking about 802.11b) He added: "Now I don't know if this technology is mature enough to be trusted for this type of thing - I guess I'll wait for the comments to come flooding in. I sincerely hope they've thought through the encryption and security issues here."
- 2002-04-26 The widespread use of "adaptive cruise technologies" to prevent automobile collisions is still well in the future, but some luxury cars such as Infiniti, Lexus, and Mercedes-Benz are now being offered with expensive options designed to allow moving vehicles to communicate with each and to detect sensors embedded in the pavement that detect the vehicle ahead either by radar or lidar (the laser-based equivalent of radar). Steven Schladover of the California Partners for Advanced Transit and Highways says: "It feels like you're in a train -- a train of cars. You don't see any separation between the vehicles, and, after a minute of feeling strange, most people relax and say, 'Oh, this is pretty nice!'" A lidar package for the Infiniti Q45 will require purchase of a \$10,000 optional equipment package. (San Jose Mercury News 26 Apr 2002)
- 2002-06-21 State police have confiscated desktop computers and hard drives at Arizona State University on the suspicion that unknown third parties installed keystroke-capture software on the computers with the goal of recording credit-card numbers and other personal data. Most of the affected systems were in open-use kiosks, according to campus representatives. The U.S. Secret Service is leading the investigation, with help from Arizona State Police. Computer systems at other colleges may also be involved. Speculation targets the Russian mafia as the perpetrators. Chronicle of Higher Education, 20 June 2002
- 2003-03-10 A Windows root kit called "ierk8243.sys" was discovered on the network of Ontario University last January. It has since been dubbed "Slanret", "IERK," and "Backdoor-ALI." A root kit is an assembly of programs that subverts the Windows operating system at the lowest levels, and, once in place, cannot be detected by conventional means. Also known as "kernel mode Trojans," root kits are far more sophisticated than the usual batch of Windows backdoor programs. Greg Hoglund, a California computer security consultant, believes intruders have been using Windows root kits covertly for years. He says the paucity of kits captured in the wild is a reflection of their effectiveness — not slow adoption by hackers. Once Slanret is installed on a hacked machine, anti-virus software won't pick it up in a normal disk scan. That said, the program is not an exploit — intruders have to gain access to the computer through some other means before planting the program. Despite their increasingly sophisticated design, the current crop of Windows root kits are generally not completely undetectable, and Slanret is no exception. Because it relies on a device driver, booting in "safe mode" will disable its cloaking mechanism, rendering its files

visible. And in what appears to be an oversight by the kit's author, the device driver "ierk8243.sys" is visible on the list of installed drivers under Windows 2000 and XP, according to anti-virus company Symantec Security Response. Høglund says future Windows root kits won't suffer from Slanret's limitations. And while he says the risk can be reduced with smart security policies — accept only digitally-signed device drivers, for one — ultimately, he worries the technique may find its way into self-propagating malicious code.

- 2004-07-26      The use of wireless networks of sensors and machinery has been expanding rapidly in such applications as the management of lighting systems and the detection of construction defects. Recent examples include a wireless communications system to tell precisely when to irrigate and harvest grapes to produce premium wine and a system to monitor stresses on aging bridges to help states decide maintenance priorities. Hans Mulder, associate director for research at Intel, says that systems such as these "will be pervasive in 20 years." Tom Reidel of Millennial Net comments: "The range of potential market applications is a function of how many beers you've had," but adds: "There's a whole ecosystem of hardware, software and service guys springing up." (New York Times 26 Jul 2004)
- 2005-01-20      Toshiba has developed software that will make it possible for people to edit documents, send e-mail, and reboot their PCs remotely from their cellphones, allowing them to work anywhere. Toshiba will begin offering the service in Japan by the end of March through CDMA1X mobile phones offered by KDDI Corp. Toshiba is initially targeting the corporate work force, but says individuals can use it to record TV shows, work security cameras and control air conditioners tied to home networks. (AP/Los Angeles Times 20 Jan 2005)

## 9 Voice Mail Security

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 US\$2.1 million.

Other cases:

- 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.

For additional reading on this topic, see

- Gerald Kovacich's article on "Voice mail security" at  
< [http://searchsecurity.techtarget.com/tip/1.289483,sid14\\_gci910850,00.html](http://searchsecurity.techtarget.com/tip/1.289483,sid14_gci910850,00.html) >
- Brian Sullivan's article, "Security experts: Voice mail is vulnerable"  
< <http://www.cnn.com/2002/TECH/ptech/04/12/voice.mail.security.idg/?related> >
- John J. Williams' textbook, *Voice Mail Security* (ISBN 0-934-27458-4, published 2000)  
< <http://www.amazon.com/exec/obidos/ASIN/0934274584/> >
- Lucie Draper's 2003 white paper, "Security in Diverse Networks: Bringing Voice and Wireless into the Fold."  
IDC Executive Brief available free from Avaya after registration  
< [http://www1.avaya.com/enterprise/whitepapers/pc/idc\\_eb327.pdf](http://www1.avaya.com/enterprise/whitepapers/pc/idc_eb327.pdf) >

## 10 Salami Fraud

Another 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. Some examples:

- 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.



## 11 Logic bombs

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. Examples of logic bombs:

- According to a report in the National Computer Security Association section on CompuServe, the Orlando Sentinel reported in January 1992 that 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.
- 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 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.

### 11.1 Time bombs

Time bombs are a subclass of logic bombs which “explode” at a certain time. 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; however, on every Friday the 13th, it also corrupted all available disks. The Michelangelo virus tried to damage hard disk directories on the 6th of March. Another common PC virus, *Cascade*, made all the characters fall to the last row of the display during the last three months of every year.

The HP3000 *ad hoc* database inquiry facility, QUERY.PUB.SYS, had a time-bomb-like bug which exploded after the 1st of January 1990. Users noticed stack overflows when trying to use certain features of the REPORT command. HP quickly sent out patches to fix the problem.

Tony Xiaotong Yu, 36, of Stamford, CT, was indicted on 2000-02-10 in NY State Supreme Court in Manhattan on charges of unauthorized modifications to a computer system and grand larceny. Mr Yu worked for Deutsche Morgan Grenfell Inc. from 1996 as a programmer. By the end of 1996, he became a securities trader. The indictment charges 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 Mr Yu allegedly inserted.<sup>5</sup>

### 11.2 Renewable software licenses

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.<sup>6</sup>

---

<sup>5</sup> Associated Press (2000). Man indicted in computer case. *New York Times*, Feb 10, 2000.

<sup>6</sup> See Internet Movie Database (IMDB), < <http://www.imdb.com/title/tt0105414/> >

In the CONSULT Forum of CompuServe in the early 1990s, several consultants brazenly admitted that they always leave secret time bombs in their software until they receive the final payment. They seemed to imply that this was a legitimate bargaining chip in their relationships with their customers.

In reality, such tricks can land software suppliers in court.

Gruenfeld (1990) reported on a logic bomb found 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.

A legitimate use similar to time-bomb technology 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, sends instructions for patching the program (that is, perform the necessary modifications) or dials up the client's system by modem and makes the patches directly.

Such a program is not technically a time bomb as long as the license contract clearly specifies that there is a time limit beyond which the program will not function properly. However, it is a poor idea for the user. In the opinion of Mr. Gruenfeld,

What if the customer is told about the bomb prior to entering into the deal? The threat of such a sword of Damocles amounts to extortion which strips the customer of any bargaining leverage and is therefore sufficient grounds to cause rejection of the entire deal. Furthermore, it is not a bad idea to include a stipulation in the contract that no such device exists.

In addition, a time-limited program can cause major problems if the vendor refuses to update the program 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. However, if you are simply renting off-the-shelf software such as utilities, accounting packages and so on, it may be acceptable to let the vendor insist on timeouts--provided the terms are made explicit and you know what you're getting into.

If you do agree to time limits on your purchase, you should require the source code to be left in escrow with a legal firm or bank. 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.

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 legally obligated to correct the time bomb and allow you to continue using your copy of the program.

### **11.3 Circumventing logic bombs**

The general class of logic bombs cannot reasonably be circumvented unless the victim can figure out exactly what conditions are causing the bomb. For example, at one time, the MPE-V operating system failed if anyone on the HP3000 misspelled a device class name in a :FILE equation. It wasn't a logic bomb, it was a bug; but the workaround was to be very careful when typing :FILE equations. I remember we put up a huge banner over the console reminding operators to double-check the spelling following the ;DEV' parameter.

Time bombs may be easier to handle than other logic bombs, depending on how the trigger is implemented. There are several methods used by programmers to implement time bombs:

- One is a simple-minded dependence on the system clock to decide if the current date is beyond the hard-coded time limit in the program file; this bomb is easily defused by resetting the system clock while one tries to solve the problem with the originator.
- The second method is a more sophisticated check of the system directory to see if any files have creation or modification dates which exceed the hard coded limit.
- The third level is to hide the latest date recorded by the program in a data file and see if the apparent date is earlier than the recorded date (indicating that the clock has been turned back).

If the time limit has been hard coded without encryption, then a simple check of the program file may reveal either ASCII data or a binary representation of the date involved. If you know what the limiting date is, you can scan for the particular binary sequence and try changing it in the executable file. These processes are by no means easy or safe, so you may want to experiment after a full backup and when no one is on the system.

If the time limit is encrypted, or if it resides in a data file, or if it is encoded in some weird aspect of the data such as the byte count of various innocuous-looking fields, the search will be impracticably tedious and uncertain.

Much better: solve your problems with the vendor before either of you declares war.

## 12 Data leakage

Information can be stolen without obvious loss; often data thefts are undiscovered until the information is used for extortion or fraud. The term *data leakage* is used to suggest the sometimes undetectable loss of control over confidential information.

The most obvious form of unauthorized disclosure of confidential or proprietary data is direct access and copying. For example, Thomas Whiteside writes that 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. Other cases of outright data theft include

- The Australian Taxation Commission, where a programmer sold documentation about tax audit procedures to help unscrupulous buyers reduce the risks of being audited
- The Massachusetts State Police, where an officer is alleged to have sold computerized criminal records
- The theft of FBI National Crime Information Center data
- The sale of records about sick people from the Norwegian Health Service to a drug company
- The misuse of voter registration lists in California, New York City, the U.S. House of Representatives and Sweden.

In June 1992, officers of the Pinellas County sheriff's office were alerted to the theft of subscribers' credit card information from the computers of Time magazine. An analyst working in the customer service offices of the publication in Tampa, Florida was arrested in July. Police found 80,000 names, credit card numbers and expiration dates on diskettes in the accused's home. As far as the police knew, the only purchasers of the data were undercover agents who bought 3,000 credit card numbers at a dollar each.

Ordinary diskettes can hold more than a megabyte of data; optical disks and special forms of diskette can hold up to gigabytes. Ensure that everyone in your offices using PCs or workstations understands the importance of securing diskettes and hard drives to prevent unauthorized copying. The effort of locking a system and putting diskettes away in secure containers under lock and key is minor compared to the possible consequences of data leakage.

Electronic mail can also be a channel for data leakage. For example, in September 1992, Borland International accused an ex-employee of passing trade secrets to its competitor--and his new employer--Symantec Corporation. The theft was discovered in records of MCI Mail electronic messages allegedly sent by the executive to Symantec.

In November 1992, NASA officials asked the FBI to investigate security at the Ames Research Center in Mountain View, California. An internal audit had revealed "major, major indication of potential violations of national security." Both the Washington Post and United Press International had stories on the problems, presumed to be cases of data leakage.

A case of data leakage via Trojan 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 US\$140 million of fraudulent long distance calls. In a significant detail, Ivy James Lay, a switch engineer working for MCI, was known in criminal hacker circles as "Knight Shadow." He was accused of having inserted Trojan horse software to record calling-card and ordinary credit-card numbers passing through MCI's telephone switching equipment. European confederates, led by 22-year old Max Louarn, of Majorca, Spain, paid him for the stolen data, then set up elaborate call centers through which users could make overseas calls.

## 12.1 Some cases of data leakage:<sup>7</sup>

- 1997-02-23 In Sheffield, England, a hospital handed over 50,000 confidential gynecological records to a data processing firm that hired people off the street and set them to work transcribing the unprotected data. The scandal resulted in withdrawal of the contract, but thousands of records were exposed to a wide variety of people with no background checking to ascertain their reliability.
- 1997-07-02 A report by Trudy Harris in *The Australian* reviewed risks of telemedicine, a technology of great value in Australia because of great distances and sparse population. Risks included interception of unencrypted medical information, modification of critical parameters for patient care, and unauthorized access to confidential patient records.
- 1997-07-10 Mark Abene, a security expert formerly known to the underground as Phiber Optik, launched a command to check a client's password files — and ended up broadcasting the instruction to thousands of computers worldwide. Many of the computers obligingly sent him their password files. Abene explained that the command was sent out because of a misconfigured system and that he had no intention of generating a flood of password files into his mailbox. Jared Sandberg, Staff Reporter for the *The Wall Street Journal*, wrote, "A less ethical hacker could have used the purloined passwords to tap into other people's Internet accounts, possibly reading their e-mail or even impersonating them online." Mr Abene was a member of the Masters of Deception gang and was sentenced to a year in federal prison for breaking into telephone company systems. The accident occurred while he was on parole.
- 1997-07-19 A firm of accountants received passwords and other confidential codes from British Inland Revenue. Government spokesmen claimed it was an isolated incident. [How exactly did they know that it was an isolated incident?]
- 1997-08-07 The ICSA's David Kennedy reported on a problem in Hong Kong, where Reuters described a slip that revealed personal details about hundreds of journalists at the end of June. Passport and identity-card details were revealed on the government Website for a couple of days. DK commented, "I suppose that's one way to get the media interested in privacy matters."
- 1997-08-15 Experian Inc. (formerly TRW Information Systems & Services), a major credit information bureau, discontinued its online access to customers' credit reports after a mere two days when at least four people received reports about other people.
- 1999-01-29 The Canadian consumer-tracking service Air Miles inadvertently left 50,000 records of applicants for its loyalty program publicly accessible on their Web site for an undetermined length of time. The Web site was offline as of 21 January until the problem was fixed.
- 1999-02-03 An error in the configuration or programming of the F. A. O. Schwarz Web site resulted paradoxically in weakening the security of transactions deliberately completed by FAX instead of through SSL. Customers who declined to send their credit-card numbers via SSL ended up having their personal details — address and so forth — stored in a Web page that could be accessed by anyone entering a URL with an appropriate (even if randomly chosen) numerical component.
- 2000-02-06 The former director of the CIA, John Deutch, kept thousands of highly classified documents on his unsecured home Macintosh computer. Critics pointed out that the system was also used for browsing the Web, opening the cache of documents up to unauthorized access of various kinds.

---

<sup>7</sup> Kabay, M. E. (2005). INFOSEC Year in Review. See < <http://www2.norwich.edu/mkabay/tyjr> > for details and instructions on downloading this free database. PDF reports are also available for download.

- 2000-02-06 An error at the Reserve Bank of Australia caused e-mail to be sent to 64 subscribers of the bank's alert service informing them of a planned 0.5% increase in the prime interest rate. However, the message was sent out six minutes early, allowing some of those traders to sell A\$3B of treasury bill and bond futures — and making some people a great deal of money.
- 2000-02-20 H&R Block had to shut down its Web-based online tax-filing system after the financial records of at least 50 customers were divulged to other customers.
- 2000-04-28 Conrad Heiney noted in RISKS that network-accessible shared trashcans under Windows NT have no security controls. Anyone on the network can browse discarded files and retrieve confidential information. [Moral: electronically shred discarded files containing sensitive data.]
- 2000-06-18 A RISKS correspondent reported on a new service in some hotels: showing the name of the guest on an LCD-equipped house phone when someone calls a room. Considering the justified reluctance to reveal the room number of a guest or to give out the name of a room occupant if one asks at the front desk, this service seems likely to lead to considerable abuse, including fraudulent charges in the hotel restaurant.
- 2000-06-24 New York Times Web-site staff chose an inappropriate mechanism for obscuring information in an Adobe Acrobat PDF document that contained information about the 1953 CIA-sponsored coup d'état in Iran. The technicians thought that adding a layer on top of the text in the document would allow them to hide the names of CIA agents; however, incomplete downloading allowed the supposedly hidden information to be read. Moral: change the source, not the output, when obscuring information.
- 2000-07-07 One of Spain's largest banks — and its most aggressive in terms of moving operations onto the Internet — is suffering from an identity crisis that has resulted in thousands of messages being routed to Bulletin Board VA, run by a rural Virginia man who publishes a weekly shopper with a circulation of 10,000. Banco Bilboa Vizcaya Argentaria, which goes by the acronym BBVA after Banco Bilbao Vizcaya merged with Argentaria SA last fall, is the owner of the "grupobbva.com" domain name, but many employees, customers and outside vendors mistakenly send their sometimes-sensitive e-mail to "bbva.com," a domain name owned by Bulletin Board VA. "When all this e-mail started coming in, I didn't know who to contact. I didn't know who to talk to," says Bulletin Board VA owner Jim Caldwell. "To me it is beyond the stage of funny." Some of the messages contain bank account numbers and balances, and at least one contained confidential information about a possible bank acquisition. BBVA says it's in the process of changing its domain name to "bbva.es," and hopes that will solve the problem. Caldwell certainly hopes so — he says he spends up to two hours a day clearing his server of the mislabeled messages. (Wall Street Journal 7 Jul 2000)
- 2000-07-13 Microsoft . . . acknowledged that a flaw in its Hotmail program . . . [was] inadvertently sending subscribers' e-mail addresses to online advertisers. The problem, which is described as a "data spill," occurs when people who subscribe to HTML newsletters open messages that contain banner ads. "The source of the problem is that Hotmail includes your e-mail address in the [Web address], and if you read an e-mail that has banner ads," the Web address will be sent to the third-party company delivering the banner, says Richard Smith, a security expert who alerted Microsoft to the problem in mid-June. Data spills are common on the Web, says Debra Pierce of the Electronic Frontier Foundation. "This isn't just local to Hotmail; we've seen hundreds of instances of data spills over the course of this year." Smith estimates that more than a million addresses may have been transferred to ad firms, but most of the big agencies, including Engage and DoubleClick, are discarding the information. (Los Angeles Times 13 Jul 2000)
- 2000-07-24 AT&T allowed extensive details of a phone account to be revealed to anyone entering a phone number into their touch-tone interface for the Credit Management Center.

- 2000-08-01 Peter Morgan-Lucas reported to RISKS, "Barclays Bank yesterday had a problem with their online banking service - at least four customers found they could access details of other customers. Barclays are claiming this to be an unforeseen side-effect of a software upgrade over the weekend."
- 2000-08-14 Kevin Poulson of SecurityFocus reported "Verizon's twenty-eight million residential and business telephone subscribers from Maine to Virginia had portions of their private telephone records exposed on a company web site. . . ." The system was designed to permit customers to file and track their repair reports, but entering any phone number generated HTML code containing the legitimate number's registered user information such as name and address.
- 2001-02-16 Paul Henry noted that the well-known problem of hidden information in MS Word documents continues to be a source of breaches of confidentiality. Writing in RISKS, he explained, "I received an MS Word document from a software start-up regarding one of their clients. Throughout the document the client was referred to as 'X', so as not to disclose the name. However I do not own a copy of Word, and was reading it using Notepad of all things, and discovered at the end the name of the directory in which the document was stored -- and also the real name of the client! I checked on a number of other word documents I had for hidden info, especially ones from Agencies who are looking to fill positions -- and yes, again I was able to tell who the client was from the hidden information in the documents." Mr Henry concluded, "Risks: What potentially damaging information is hidden in published documents in Word, PDF and other complex formats? Mitigation: Use RTF when you can -- no hidden info, no viruses."
- 2001-06-22 The e-mail of Dennis Tito, the investment banker who paid to become the first tourist in space, was insecure for more than a year -- as were the communications of his entire company, Wilshire Associates. . . . Although there is no evidence that anyone took advantage of the breaches, they allowed access by outsiders to confidential company business, including financial data, passwords, and the personal information of employees. However, security experts say Wilshire's problem is not an isolated one, and warn that American companies are not taking computer security issues seriously. Peter G. Neumann, principal scientist in the computer science lab at SRI International, says that the security breach discovered at Wilshire is just "one of thousands of vulnerabilities known forever to the world. Everybody out there is vulnerable." (Washington Post 22 Jun 2001)
- 2001-07-05 The drug company Eli Lilly sent out an e-mail reminder to renew their prescriptions for Prozac to 600 clients -- and used CC instead of BCC, thus revealing the entire list of names and e-mail addresses to all 600 recipients.
- 2001-11-26 Search engines increasingly are unearthing private information such as passwords, credit card numbers, classified documents, and even computer vulnerabilities that can be exploited by hackers. "The overall problem is worse than it was in the early days, when you could do AltaVista searches on the word 'password' and up come hundreds of password files," says Christopher Klaus, founder and CTO of Internet Security Systems, who notes that a new tool built into Google to find a variety of file types is exacerbating the problem. "What's happening with search engines like Google adding this functionality is that there are a lot more targets to go after." Google has been revamped to sniff out a wider array of files, including Adobe PostScript, Lotus 1-2-3, MacWrite, Microsoft Excel, PowerPoint, Word, and Rich Text Format. Google disavows responsibility for the security problem, but the company is working on ways to limit the amount of sensitive information exposed. "Our specialty is discovering, crawling and indexing publicly available information," says a Google spokesman. "We define 'public' as anything placed on the public Internet and not blocked to search engines in any way. The primary burden falls to the people who are incorrectly exposing this information. But at the same time, we're certainly aware of the problem, and our development team is exploring different solutions behind the scenes." (CNET News.com 26 Nov 2001)

- 2002-02-20 RISKs correspondent Diomidis Spinellis cogently summarized some of the problems caused by search engines on the Web: “The aggressive indexing of the Google search engine combined with the on-line caching of the pages in the form they had when they were indexed, is resulting in some perverse situations. A number of RISKs articles have already described how sensitive data or supposedly non-accessible pages leaked from an organization’s intranet or web-site to the world by getting indexed by Google or other search engines. Such problems can be avoided by not placing private information on a publicly accessible web site, or by employing metadata such as the robot exclusion standard to inform the various web-crawling spiders that specific contents are not to be indexed. Of course, adherence to the robot exclusion standard is left to the discretion of the individual spiders, so the second option should only be used for advisory purposes and not to protect sensitive data.”
- 2002-03-22 Paul van Keep reported in RISKs, >Christine Le Duc, a dutch chain of s\*xshops, and also a mail & Internet order company, suffered a major embarrassment last weekend. A journalist who was searching for information on the company found a link on Google that took him to a page on the Web site with a past order for a CLD customer. He used the link in a story for online newspaper nu.nl. The full order information including name and shipping address was available for public viewing. To make things even worse it turned out that the classic URL twiddling trick, a risk we’ve seen over and over again, allowed access to ALL orders for all customers from 2001 and 2002. The company did the only decent thing as soon as they were informed of the problem and took down the whole site.<  
[Note: \* included to foil false positive exclusion by crude spam filters.]
- 2002-06-10 Monty Solomon wrote in RISKs, “A design flaw at a Fidelity Investments online service accessible to 300,000 people allowed Canadian account holders to view other customers’ account activity. The problem was discovered over the weekend by Ian Allen, a computer studies professor at Algonquin College in Ottawa. Fidelity said it had fixed the problem and was offering customers the option of changing account numbers.”
- 2003-01-16 MIT graduate students Simson Garfinkel and Abhi Shelat bought 158 hard drives at second hand computer stores and eBay over a two-year period, and found that more than half of those that were functional contained recoverable files, most of which contained “significant personal information.” The data included medical correspondence, love letters, pornography and 5,000 credit card numbers. The investigation calls into question PC users’ assumptions when they donate or junk old computers — 51 of the 129 working drives had been reformatted, and 19 of those still contained recoverable data. The only surefire way to erase a hard drive is to “squeeze” it — writing over the old information with new data, preferably several times — but few people go to the trouble. The findings of the study will be published in the IEEE Security & Privacy journal Friday. (AP 16 Jan 2003)
- 2003-02-10 A state auditor found that at least one computer used by staffers counseling clients with AIDS or HIV was ready to be offered for sale to the public even though it still contained files of thousands of people. Auditor Ed Hatchett said: “This is significant data. It’s a lot of information lots of names and things like sexual partners of those who are diagnosed with AIDS. It’s a terrible security breach.” Health Services Secretary Marcia Morgan, who has ordered an internal investigation of that breach, says the files were thought to have been deleted last year. (AP/USA Today 7 Feb 2003)
- 2003-04-17 A glitch on the CNN.com Web site accidentally made available draft obituaries written in advance for Dick Cheney, Ronald Reagan, Fidel Castro, Pope John Paul II and Nelson Mandela. “The design mockups were on a development site intended for internal review only,” says a CNN spokeswoman. “The development site was temporarily publicly available because of human error.” The pages were yanked about 20 minutes after being exposed. (CNet News.com 17 Apr 2003)”



- 2003-05-29 Hacker Adrian Lamo found a security hole in a website run by lock\line LLC, which provides claim management services to Cingular customers. Lamo discovered the problem last weekend through a random finding in a Sacramento, CA dumpster, where a Cingular store had discarded records about a customer's insurance claim for a lost phone. By simply typing in a URL listed on the detritus, Lamo was taken to the customer's claim page on the lock\line website. Lamo was able to access individual claims pages containing customer's name, address and phone number, along with details on the insurance claim being made. Altering the claim ID numbers in the URL gave Lamo access to some 2.5 million Cingular customer claims dating back to 1998. Lamo said he had no intent of profiting from the exploit, just pointing out a security flaw. Cingular and lock\line closed the hole by Wednesday morning.
- 2003-06-16 Confidential vulnerability information managed by the CERT Coordination Center has again been leaked to the public. The latest report was posted to a vulnerability discussion list by an individual using the name "hack4life." The latest information concerns a flaw in Adobe Systems Inc.'s PDF (Portable Document Format) readers for Unix and could allow a remote attacker to trick users into executing malicious code on their machines, according to a copy of the leaked vulnerability report. The leaked information was taken from communication sent from CERT to software vendors affected by the PDF problem, according to Jeffrey Carpenter, manager of the CERT Coordination Center. The information appears to be from a vulnerability report submitted to CERT by a Cincinnati security researcher by the name of Martyn Gilmore. Adobe's Acrobat Reader 5.06 and the open-source reader Xpdf 1.01 are affected by the problem, according to the report.
- 2003-06-30 Pet supply retailer PetCo.com plugged a hole in its online storefront over the weekend that left as many as 500,000 credit card numbers open to anyone able to construct a specially-crafted URL. Twenty-year old programmer Jeremiah Jacks discovered the hole. He used Google to find active server pages on PetCo.com that accepted customer input and then tried inputting SQL database queries into them. "It took me less than a minute to find a page that was vulnerable," says Jacks. The company issued a statement Sunday saying it had hired a computer security consultant to assist in an audit of the site."
- 2003-09-15 Two Bank of Montreal computers containing hundreds, potentially thousands, of sensitive customer files narrowly escaped being sold on eBay.com late last week, calling into question the process by which financial institutions dispose of old computer equipment. Information in one of the computers included the names, addresses and phone numbers of several hundred bank clients, along with their bank account information, including account type and number, balances and, in some cases, balances on GICs, RRSPs, lines of credit, credit cards and insurance. Many of the files were dated as recently as late 2002, while some went back to 2000. The computers appeared to originate from the bank's head office on St. Jacques St. in Montreal, but customers, many of them also bank employees, had addresses ranging from Victoria, B.C., to St. John's, Nfld.
- 2004-01-05 Contributor Theodor Norup reports that a press-release Word document from the Danish Prime Minister's Office unintendedly revealed its real source and all its revisions. As a result of this incident, ministry spokesman Michael Kristiansen said the Prime Minister's office would "distribute speeches as PDF files..." Norup believes the risk still is trusting "high echelons of governments" will know a little about information security.
- 2004-03-16 A portion of Windows source code was leaked last month, and researchers are saying that hackers have uncovered several previously unknown vulnerabilities in the code. Immediately following the code's posting on the Internet, members of the security underground began poring over the code, searching for undocumented features and flaws that might give them a new way to break into Windows machines. The real danger isn't the vulnerabilities that this crowd finds and then posts; it's the ones that they keep to themselves for personal use that have researchers worried. Experts said there has been a lot of talk about such finds on hacker bulletin boards and Internet Relay Chat channels of late, indicating that some hackers are busily adding new weapons to their armories. Another concern for Microsoft and its customers is that even though the leaked code is more than

10 years old, it forms the base of the company's current operating system offerings, Windows XP and Windows Server 2003. This means that any vulnerabilities found in Windows NT or Windows 2000 could exist in the newer versions as well.

- 2004-10-19 Google Desktop Search may prove a boon to disorganized PC users who need assistance in finding data on their computers, but it also has a downside for those who use public or workplace computers. Its indexing function may compromise the privacy of users who share computers for such tasks as processing e-mail, online shopping, medical research, banking or any activity that requires a password. "It's clearly a very powerful tool for locating information on the computer," says one privacy consultant. "On the flip side of things, it's a perfect spy program." The program, which is currently available only for Windows PCs, automatically records any e-mail read through Outlook, Outlook Express or the Internet Explorer browser, and also saves pages viewed through IE and conversations conducted via AOL Instant Messenger. In addition, it finds Word, Excel and PowerPoint files stored on the computer. And unlike the built-in cache of recent Web sites visited that's included in most browser histories, Google's index is permanent, although individuals can delete items individually. Acknowledging potential privacy concerns, a Google executive says managers of shared computers should think twice about installing the tool before advanced features like password protection and multi-user support are available.
- 2005-02-07 A leaked list containing the names of about 240,000 people who allegedly spied for Poland's former communist regime has overtaken sex as the hottest search item on the Net in Poland. "This thing is huge. We have recorded around 100,000 Internet searches a day for the list, which is 10 times the number looking for sex," Piotr Tchorzewski, who works at Poland's biggest Internet portal Onet, told Rzeczpospolita Daily. The list, which contains in alphabetical order the names of alleged agents and collaborators of the communist-era secret service, mixed together with the names of those who were allegedly spied on, has also been put up for auction on the Internet, but its bid price late today -- 2.99 zlotys (about \$AU1.25) -- was hardly breaking records. (The Australian 7 Feb 2005)
- 2005-02-18 ChoicePoint, a spinoff of credit reporting agency Equifax, has come under fire for a major security breach that exposed the personal data records of as many as 145,000 consumers to thieves posing as legitimate businesses. The information revealed included names, addresses, Social Security numbers and credit reports. "The irony appears to be that ChoicePoint has not done its own due diligence in verifying the identities of those 'businesses' that apply to be customers," says Beth Givens, director of the Privacy Rights Clearinghouse. "They're not doing the very thing they claim their service enables their customers to achieve." In its defense, ChoicePoint claims it scrutinizes all account applications, including business license verification and individuals' background checks, but in this case the fraudulent identities had not been reported stolen yet and everything seemed in order. ChoicePoint marketing director James Lee says they uncovered the deception by tracking the pattern of searches the suspects were conducting. (Washington Post 18 Feb 2005)
- 2005-04-07 A hard drive full of confidential police data has been sold on eBay, for only \$25. Germany's Spiegel newspaper reported earlier this week that the 20GB hard drive contained a raft of information about Brandenburg police, including details of political security situations. "This week's exposure of leaked and highly critical information from the Brandenburg police in Germany reinforces how important it is to never let mobile devices or hard drives leave the office without being adequately protected with encryption and strong password protection — even after they have been discarded," said Peter Larsson, CEO of mobile technology company Pointsec. The drive was eventually bought by a student from Potsdam who alerted police once he realized what it contained.

## 12.2 USB Flash Drives

John Bumgarner (President of Cyber Watch, Inc.) and I published the following summary of data leakage risks from USB flash drives in Network World Fusion in 2003

< <http://www.nwfusion.com/newsletters/sec/2003/1027sec1.html> > and

< <http://www.nwfusion.com/newsletters/sec/2003/1027sec2.html> >:

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 computer 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.

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.

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> >.

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](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.

### **12.3 Surveillance**

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](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.

## 12.4 Steganography

Unfortunately, there are more subtle ways of stealing information. Security specialists have long pointed out that information can be carried in many ways, not just through obvious printed copies or outright copies of files. For example, a programmer may realize that (s)he will not have access to production data, but the programmer's programs will. So (s)he 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."

For more information about steganography, see

- Fabien Petitcolas' "Information hiding home page / digital watermarking & steganography" < <http://www.petitcolas.net/fabien/steganography/> >
- Peter McGrath's article on "Coded Communications" (2001) < <http://msnbc.msn.com/id/3067670/> >
- Wiretapped's list of stego products < <http://www.wiretapped.net/indexes/steganography.html> >
- INFOSYSSEC's list of tutorials, articles, FAQs and reviews < <http://www.infosyssec.com/infosyssec/stendig1.htm> >

## 12.5 Inference

Charles Pfleeger points out that even small amounts of information can sometimes be valuable; e.g., the mere existence of a specific named file may tell someone what they need to know about a production process. Such small amounts of information can be conveyed by any 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.

## 12.6 Plugging covert channels

Alas, there are many subtle ways of stealing information. 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 (but 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.

Even without data processing equipment, one can ferry information out of a secured system using photography. A search for "spy cameras" on GOOGLE brings up many hits for tiny, concealable cameras— and today we find cameras even in mobile phones.

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.

Again, the best defense starts with the educated, security-conscious employee.

## 13 Extortion

Computer data can be held for ransom. For example, according to Whiteside,

- 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.

### 13.1 More recent cases:<sup>8</sup>

- 1999-10-15      Jahair Joel Navarro, an 18-year-old from New York state, was indicted in White Plains on charges of extortion. He allegedly threatened to bomb Microsoft and IBM headquarters unless each company paid him \$5M. An FBI raid on the lad's apartment found no bombs but only the usual instructions on bomb-making downloaded from the Internet.
- 2000-01-12      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.
- 2000-01-15      In September 1999, the Sunday Times reported in an article by Jon Ungood-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. Ungood-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

---

<sup>8</sup> Kabay, M. E. (2005). INFOSEC Year in Review. See < <http://www2.norwich.edu/mkabay/iyjr> > for details and instructions on downloading this free database. PDF reports are also available for download.



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.” According to Padraic Flanagan of the British Press Association in mid-January 2000, UK police were investigating a dozen attempts by criminal hackers to extort funds from multinational companies in Britain.

- 2000-01-18 In January, information came to light that VISA International had been hacked by an extortionist who demanded \$10M for the return of stolen information — information that VISA spokesperson Chris McLaughlin described as worthless and posing no threat to VISA or to its customers. The extortion was being investigated by police but no arrests had been made. However, other reports suggested that the criminal hackers stole source code and could have crashed the entire system. In a follow-up on RISKS, a correspondent asked, “. . . [What source code was \*stolen\*? It is extremely unlikely that it was \*the source code for the Visa card system\* as stated! There is no such thing. Like any system, it would consist of many source libraries, each relating to different modules of the overall system. So we should be asking what source was copied? (You can hardly say it was \*stolen\*, as that would imply that it was taken away, leaving the rightful owner without possession of the item of stolen property, and we all know that is not what happens in such cases. In a shop like Visa, the code promotion system maintains multiple copies in the migration libraries, so erasure of the sole copy is highly unlikely).”
- 2000-01-25 French programmer Serge Humpich spent four years on the cryptanalysis of the smart-card authentication process used by the Cartes Bancaires organization and patented his analysis. When he demonstrated his technique in September 1999 by stealing 10 Paris Metro tickets using a counterfeit card, he was arrested. The man had asked the credit-card consortium to pay him the equivalent of \$1.5M for his work; instead, he faced a seven-year term in prison and a maximum fine of about \$750,000 for fraud and counterfeiting (although prosecutors asked for a suspended sentence of two years’ probation and a fine of approximately US\$10,000). He was also fired from his job because of the publicity over his case. In late February 2000, he was given a 10-month suspended sentence and fined 12,000 FF (~US\$1,800).
- 2000-12-13 The FBI . . . [began] searching for a network vandal who stole 55,000 credit card numbers from a private portion of the Creditcards.com Web site and published them on the Internet after the company refused to pay the intruder money in order to keep the information from being circulated. . . .” (New York Times 13 Dec 2000) The attack began in August 2000 but the revenge posting of the numbers occurred only in December. The criminal demanded \$100,000 in extortion money and also claimed on a Web site that he was trying to obtain a contract for improving network security: “Michael Butts says I need to talk to Michael Stankewitz from COO [sic]...I told him that I want to help creditcards.com, he had my price and he knew my deal,” the Web page reads. “He knew what kind of information we had from their servers. I would destroy it all after the agreement was made and provide network security. Now, I didn’t receive any payment from creditcards.com and I am going to make them bankrupt.”
- 2001-03-02 The FBI says an organized ring of hackers based in Russia and the Ukraine has stolen more than a million credit card numbers from 40 sites in 20 states over the last few months, and attempted to blackmail the targeted businesses by threatening to embarrass them publicly. The intrusions have been made using a well-known vulnerability that existed in the Windows NT operating system. Free patches to prevent intrusion can be found at [www.microsoft.com](http://www.microsoft.com). (Washington Post 9 Mar 2001)
- 2001-03-09 A little-known company called TechSearch has found a new gimmick for making money off the Net -- it’s 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. “We chose to settle the lawsuit rather than move forward with potentially costly

litigation,” says a Britannica spokeswoman. Following complaints that the patent is invalid, the U.S. Patent and Trademark Office reached an initial decision late last month to void it, but TechSearch has amassed a collection of 20-some other patents that it can use to extract payments. It’s filed several lawsuits against major electronics firms based on a 1986 patent on “plug and play” technology, and has initiated litigation with several distance learning providers based on a 1989 patent that broadly covers computer-based educational techniques. TechSearch founder Anthony Brown says his methods, although aggressive, are perfectly legal, and the company’s law firm says it’s won \$350 million in settlements in a string of jury verdicts over the last six years. Critics have labeled the company’s techniques “extortionate” and “patentmail.” (Wall Street Journal 9 Mar 2001)

- 2002-06-18 The administrator of South Africa’s web addresses said on Thursday he had hidden the key to the country’s “.ZA” domain network abroad to prevent any government interference in access to the Internet. South Africa’s parliament has given initial approval to a law that will allow the government to take control of the country’s Internet address administration. But critics, including ZA domain-name administrator Mike Lawrie, say the government has no right to stage the takeover and warn it could collapse the domestic Internet structure.
- 2003-07-29 An unanticipated by-product of Malaysia’s campaign against the sale of illegal video discs is the rise of extortionists who impersonate law enforcement officers on surprise checks and demand 50 ringgit (US\$13) for each illegal disc they find. Illegal copying of movies and computer software is pervasive in Malaysia and cheap versions of the latest Hollywood, Indian and Hong Kong films have been widely available at street stalls and in stores. (AP/San Jose Mercury News 29 Jul 2003)
- 2003-08-25 In June 2003, a high-tech extortionist in the Netherlands threatened to poison the products of the Campina food company in Utrecht unless he were paid €200,000. The steps for payment used an unusual degree of technical sophistication:
1. Campina had to open a bank account and get a credit card for it.
  2. The victims deposited the payoff in the bank account.
  3. They had to buy a credit card reader and scan the credit card to extract the data from the magnetic strip.
  4. Using a steganography program and a picture of a red VW car sent by the criminal, the victims encoded the card data and its PIN into the picture using the steganographic key supplied with the software.
  5. They then posted the modified picture in an advertisement on a automobile-exchange Web site.
  6. The criminal used an anonymizing service called SURFOLA.COM to mask his identity and location while retrieving the steganographic picture from the Web site.
- The victims worked with their local police, who in turn communicated with the FBI for help. The FBI were able to find the criminal’s authentic e-mail address along with sound financial information from his PAYPAL.COM account. Dutch police began surveillance and were able to arrest the 45-year-old micro chip designer when he withdrew money from an ATM using the forged credit card.
- 2004-02-26 Tokyo Metropolitan Police arrested three men on suspicion of trying to extort up to 3 billion yen (U.S. \$28 million) from Softbank. The suspects claimed that they obtained DVD and CD disks filled with 4.6 million Yahoo BB customer information. Two of the suspects run Yahoo BB agencies which sells DSL and IP Telephone services.... According to Softbank, the stolen data includes name, address, telephone number, and e-mail. No billing or credit card information was leaked. However, there were indications that the suspects could be linked to organized crime (the Yakuza).
- 2004-03-23 Federal law enforcement officials in California have arrested a 32-year-old man who demanded \$100,000 from Google Inc. and threatened to “destroy” the company by using a software program to fake traffic on Internet ads. The man’s program automated phony traffic to cost-per-click ads Google places on websites and caused Google to make payments to Web sites the man

had set up. Released on \$50,000 bail, he faces up to 20 years in prison and a \$250,000 fine. (Bloomberg News/Los Angeles Times 23 Mar 2004)

- 2004-05-26      Australians are being targeted by Eastern European organized crime families using the internet to extort and steal far from home. Delegates at the annual AusCERT Asia Pacific Internet Security Conference were warned Wednesday, May 26, that mobsters were hiring computer programmers to take their brand of criminal activity online. The deputy head of Britain's National Hi-Tech Crime Unit, Superintendent Mick Deats, said one Eastern European syndicate with interests in prostitution, drugs and gun smuggling was also earning money all over the world from internet credit card fraud, software piracy, child pornography and online extortion. "Australia is a focus of a lot of the phishing activity at the moment," Deats said. "The people we've arrested in London were sending money to the same people that are receiving money from attacks that are happening in Australia." Another tactic linked to several eastern European crime syndicates was using distributed denial of service attacks — bombarding online businesses with a flood of requests aimed at overloading systems and shutting them down. The businesses were then told to pay \$50,000 to make the attacks go away, he said.
- 2004-05-31      Police have arrested two additional people on suspicion of trying to extort money from Softbank after obtaining personal data on as many as 4 million subscribers to the Internet company's broadband service. The two -- Yutaka Tomiyasu, 24, and Takuya Mori, 35 -- are accused of obtaining company passwords to hack into Softbank's database from an Internet cafe in Tokyo in January, according to a Tokyo Metropolitan Police spokesman. The two allegedly passed the information to members of a right-wing extremist group, police said. Four members of the extremist group were arrested in February for allegedly threatening to publicly release the information unless Softbank paid them ¥1 billion to ¥2 billion (\$US13 million to \$US26 million). (The Australian 31 May 2004) rec'd from John Lamp, Deakin U.

## **13.2 Defenses**

Clearly, one of the best defenses against extortion based on theft of data is to have adequate backups. Another is to encrypt sensitive data so they cannot be misused even if they're stolen.

A Public Broadcasting System (PBS) television show in early 1993 reported that there are rumors that unscrupulous auditors have occasionally blackmailed white collar criminals found during audits.

The best way to prevent embarrassment or blackmail during an audit is to run internal audits. Support your internal audits staff. Explain to them what you need to protect. Point out weak areas. Better to have an internal audit report that supports your recommendations for improved security than to have a breach of security cost your employer reputation and money.

Another form of extortion is used by dishonest employees who are found out by their employers. When confronted with their heinous deeds, they coolly demand a letter of reference to their next victim. Otherwise they will publicize their own crime to embarrass the their employer. Many organizations are thought to have acceded to these outrageous demands. Some scoundrels have even asked for severance pay--and, rumor has it, they have been paid.

Such narrow defensive strategies are harming society's ability to stop computer crime.

Hiding a problem makes it worse. A patient who conceals a cancer from doctors will die sooner rather than later. Organizations that conceal system security breaches make it harder for all system managers to fight such attacks. Victims should report these crimes to legal authorities and should support prosecution.

Interestingly, there's a different kind of extortion that involves vendors and vulnerabilities. In this scam, a criminal discovers a vulnerability in a product and threatens to reveal it unless they're paid money to conceal it. The normal response of a company with any sense at all is "Publish and be damned."

## 14 Forgery

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.

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.

### 14.1 Desktop forgery

But things are getting worse. Forgers have gone high-tech. It seems nothing is sacred any more, not even certificates and signatures.

A fascinating article in *Forbes Magazine* in 1989 showed how the writer was able to use desktop publishing (DTP) equipment even that long ago to create fraudulent checks. He used a high-quality scanner, a PC with good DTP and image-enhancement (touch-up) programs and high-resolution laser printers. Color copiers and printers have opened up an even wider field for forgery than the monochrome copiers and printers did. The total cost of a suitable forgery system at this writing (July 2004) is about \$1,000 in all.

The *Forbes* article and other security references list many examples of computer-related forgeries. 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 even managed to effect their own release by sending a FAX of a forged document to their prison officers.

In December 1992, California State Police in Los Angeles 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.

You should verify the authenticity of documents before acting on them. 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.

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.

## 14.2 Fake credit cards

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.

The Internet RISKS bulletin distributed a note in December 1992 about credit card fraud. A correspondent reported on two bulletins he had noticed at a local bookstore. The first dealt with magnetically forged cards. The magnetic stripe on these fraudulent cards 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 bears the burden of the theft by paying higher credit card fees.

In one of my classes, a security officer from a large national bank explained that when interest rates on unpaid balances were at 18%, almost half of that rate (8%) was assigned to covering losses and frauds.

In January 1993, a report on the Reuter news wire indicated that credit card forgery was rampant in southeast Asia. Total losses worldwide reached \$1 billion in 1991, twice the theft in 1990. In a single raid in Malaysia in August 1992, police found 2,092 fake cards simulating MasterCard, VISA and American Express. The use of digitized photographs embedded in the cards themselves will help make counterfeiting more difficult. Statistics from the Internet Fraud Complaint Center < <http://www.ifccfbi.gov/strategy/statistics.asp> > showed drastic increases in fraud between its opening in 2000 and the latest report (2002) available at the time of writing (July 2004):

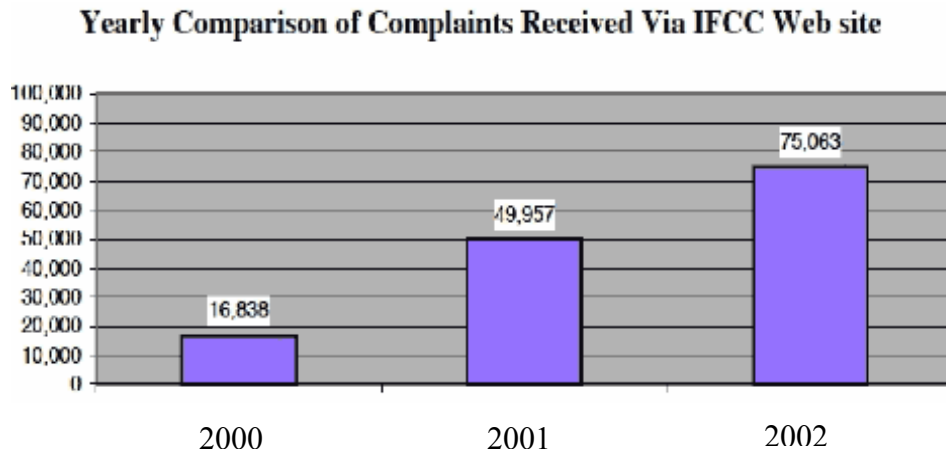


Figure 1. IFCC complaints (from <http://www.merchant911.org/fraud-trends.html> )

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.

Ultimately, it may become cost-effective to insist on the same, rather modest, level of security for credit cards as for bank cards: at least a PIN (personal identification number) to be entered by the user at the time of payment. There are, however, difficulties in ensuring the confidentiality of such PINs during telephone ordering. A solution to this problem is variable PINs generated by a "smart card:" a micro-processor-equipped credit card which generates a new PIN every minute or so. The PIN is cryptographically related to the card serial number and to the precise date and time; even if a particular PIN is overheard or captured, it is useless a very short time after the transaction. Combined with a PIN to be remembered by the user, this system may greatly reduce credit-card fraud.

## 15 Simulation

Using computers in carrying out crime is nothing new. Organized crime uses computers all the time, according to August Bequai. He catalogs applications of computers in gambling, prostitution, drugs, pornography, fencing, 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.”

If it is known that you will carry out periodic audits of files on your enterprise computer systems, there’s a better chance that you will prevent criminals from using your property in carrying out their crimes. On the other hand, such audits may force people into encrypting incriminating files. Audits may also cause morale problems, so it’s important to discuss the issue with your staff before imposing such routines.

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. Now, 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. The scheme would have worked if the computer hadn’t broken down. Scotland Yard were alerted to a rash of bad checks all over London. They traced the conspirators back to a back room where a computer programmer was desperately trying to fix his broken computer system. He had no backup hardware.

## 16 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> >
- Bequai, A. (1987). *Technocrimes: The Computerization of Crime and Terrorism*. Lexington Books (Lexington, MA). ISBN 0-669-13842-8.
- Bosworth, S. & M. E. Kabay (2002), eds. *Computer Security Handbook, 4th Edition*. Wiley (New York). ISBN 0-471-41258-9. 1184 pp. Index.
- Bullfinch, T. (1855). *The Age of Fable*. Reprinted in *Bullfinch's Mythology* in the Modern Library edition. Random House (New York).
- 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](http://www.cultdeadcow.com/news/back_orifice.txt) >
- Kabay, M. E. (2001). Fighting DDoS, part 1 (2001-07-25)  
<http://www.nwfusion.com/newsletters/sec/2001/00918845.html>
- Kabay, M. E. (2005). INFOSEC Year in Review. See < <http://www2.norwich.edu/mkabay/iyir> > for details and instructions on downloading this free database. PDF reports are also available for download.
- 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> >
- Parker, D. B. (1998) *Fighting Computer Crime: A New Framework for Protecting Information*. John Wiley & Sons (NY) ISBN 0-471-16378-3. xv + 500 pp; index
- PestPatrol Resources < <http://www3.ca.com/securityadvisor/pest/> >
- PestPatrol White Papers < <http://www3.ca.com/securityadvisor/pest/collaterallist.aspx?typeid=4> >
- 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> >
- Schwartau, W. (1991). *Terminal Compromise* (novel). Inter.Pact Press (Seminole, FL). ISBN 0-962-87000-5.
- Stoll, C. (1989). *The Cuckoo's Egg: Tracking a Spy through the Maze of Computer Espionage*. Pocket Books (New York). ISBN 0-671-72699-9.
- 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> >



Whiteside, T. (1978). *Computer Capers: Tales of Electronic Thievery, Embezzlement, and Fraud*. New American Library (New York). ISBN 0-45162080-1.

Schwartau, W. (1994). *Information Warfare: Chaos on the Electronic Superhighway*. Thunder's Mouth Press, New York. ISBN 1-56025-080-1. 432. Index